IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

RMAIL LTD., *Plaintiff,*	§	
v.	§	CASE NO. 2:10-CV-258-JRG
	§	(Lead Case)
AMAZON.COM, INC., et al., *Defendants*.	§	
_____	§	
RPOST HOLDINGS, INC., et al., *Plaintiffs,*	§	
v.	§	CASE NO. 2:11-CV-16-JRG
READNOTIFY.COM PTY LTD., et al., *Defendants*.	§	
_____	§	
RPOST HOLDINGS, INC., et al., *Plaintiffs,*	§	
v.	§	CASE NO. 2:11-CV-64-JRG
ZIX CORP., et al., *Defendants*.	§	
_____	§	
RMAIL LTD., et al., *Plaintiffs,*	§	
v.	§	CASE NO. 2:11-CV-299-JRG
DOCUSIGN, INC., et al., *Defendants*.	§	
_____	§	

	§	
	§	
RMAIL LTD., et al., *Plaintiffs*,	§	
	§	
	§	
v.	§	CASE NO. 2:11-CV-300-JRG
	§	
RIGHTSIGNATURE, LLC, et al., *Defendants*.	§	
	§	
	§	
RPOST HOLDINGS, INC., et al., *Plaintiffs*,	§	
	§	
	§	
v.	§	CASE NO. 2:11-CV-325-JRG
	§	
ADOBE SYSTEMS INC., et al., *Defendants*.	§	
	§	

MEMORANDUM OPINION AND ORDER

Before the Court is Plaintiffs'[1] Opening Claim Construction Brief (Dkt. No. 251).[2] Also before the Court is Defendants'[3] Consolidated Responsive Claim Construction Brief (Dkt. No. 253), as well as Plaintiffs' reply (Dkt. No. 257). The Court held a claim construction hearing on February 14, 2013.

[1] Plaintiffs in the lead case and the consolidated cases, collectively, are RMail Ltd., RPost Holdings, Inc., RPost International Ltd., and RPost Communications Ltd. Plaintiffs are sometimes referred to collectively as "RPost."

[2] References to documents herein shall be to docket numbers in the lead case, No. 2:10-CV-258.

[3] Defendants in the lead case and the consolidated cases, collectively, are Farmers Group, Inc. and Farmers Insurance Company, Inc. ("Farmers"), Amazon.com, Inc. ("Amazon"), PayPal Inc. ("PayPal"), ReadNotify.com PTY Ltd. ("ReadNotify"), Chris Drake, Zix Corp. ("Zix"), DocuSign, Inc. ("DocuSign"), RightSignature, LLC ("RightSignature"), Adobe Systems Inc. ("Adobe"), and EchoSign, Inc. ("EchoSign").

Table of Contents

I. BACKGROUND

Plaintiffs bring suit alleging infringement of two groups of patents, both of which relate to technologies for providing proof of message transmission, delivery, and content, such as for e-mail.

The so-called "Feldbau Patents" are United States Patents No. 6,182,219 ("the '219 Patent") and 6,571,334 ("the '334 Patent"). The '334 Patent is a continuation of the '219 Patent. The '219 Patent is the only patent-in-suit that is asserted against all of the Defendants in the above-captioned consolidated cases. A chart of which Feldbau Patent claims are asserted against each Defendant is included with the parties' January 31, 2013 P.R. 4-5(d) Joint Claim Construction Chart. (Dkt. No. 259, at 7.)

The so-called "Tomkow Patents" are United States Patents No. 7,707,624 ("the '624 Patent"), 7,865,557 ("the '557 Patent"), and 7,966,372 ("the '372 Patent"). The '557 Patent is a divisional of the '372 Patent.

The Feldbau Patents and the Tomkow Patents may be referred to collectively as "the patents-in-suit." A chart of which claims of the patents-in-suit are asserted against each Defendant is attached to Plaintiffs' opening claim construction brief. (Dkt. No. 251, at Ex. 11.)

The '219 Patent was construed by Judge James Selna of the Central District of California in *Propat Int'l Corp. v. RPost Inc., et al.*, No. SACV 03-1011-JVS(Mcx), Dkt. No. 191, 2005 WL 6287844 (C.D. Cal. Jan. 14, 2005) ("*Propat*") (attached as Exhibit 5 to Plaintiffs' opening brief in the above-captioned case).[4] All substantive rulings in the *Propat* case were subsequently vacated, however, when the court found that the plaintiff, Propat International Corp., lacked standing. No. SACV 03-1011-JVS(Mcx), Dkt. No. 338, 2005 WL 6233792 (C.D. Cal. Nov. 28,

[4] Citations to *Propat* herein shall be to the page numbers of the slip opinion.

2005) (granting motion to dismiss *with* prejudice), *amended*, Dkt. No. 339 (C.D. Cal. Nov. 30, 2005) (granting motion to dismiss *without* prejudice); Final Judgment Dismissing Action Without Prejudice, *id.*, Dkt. No. 343, at 2, ¶ 3. In short, the inventors, Ofra Feldbau and Michael Feldbau, had assigned their interest to Authentix-Authentication Technologies Ltd. ("Authentix"), which in had turn granted an exclusive license and right to enforce to Propat International Corp. *Id.*, Dkt. No. 339, slip op. at 1-2. The court found that Authentix retained substantial rights and that Propat International Corp. held only a "bare license," which left it without standing to bring suit, even if Authentix were joined. *Id.* at 5. The court therefore dismissed the case without prejudice. *Id.* at 7. The Court of Appeals for the Federal Circuit affirmed. *Propat Int'l Corp. v. RPost Inc.*, 473 F.3d 1187, 1194 (Fed. Cir. 2007).

The '219 Patent was the subject of reexamination proceedings, and a reexamination certificate issued on June 19, 2012, amending various claims of the '219 Patent. The related '334 Patent is the subject of ongoing reexamination proceedings.

II. LEGAL PRINCIPLES

It is understood that "[a] claim in a patent provides the metes and bounds of the right which the patent confers on the patentee to exclude others from making, using or selling the protected invention." *Burke, Inc. v. Bruno Indep. Living Aids, Inc.*, 183 F.3d 1334, 1340 (Fed. Cir. 1999). Claim construction is clearly an issue of law for the court to decide. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 970-71 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996).

To ascertain the meaning of claims, courts look to three primary sources: the claims, the specification, and the prosecution history. *Markman*, 52 F.3d at 979. The specification must contain a written description of the invention that enables one of ordinary skill in the art to make and use the invention. *Id.* A patent's claims must be read in view of the specification, of which

they are a part. *Id.* For claim construction purposes, the description may act as a sort of dictionary, which explains the invention and may define terms used in the claims. *Id.* "One purpose for examining the specification is to determine if the patentee has limited the scope of the claims." *Watts v. XL Sys., Inc.*, 232 F.3d 877, 882 (Fed. Cir. 2000).

Nonetheless, it is the function of the claims, not the specification, to set forth the limits of the patentee's invention. Otherwise, there would be no need for claims. *SRI Int'l v. Matsushita Elec. Corp.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985) (en banc). The patentee is free to be his own lexicographer, but any special definition given to a word must be clearly set forth in the specification. *Intellicall, Inc. v. Phonometrics, Inc.*, 952 F.2d 1384, 1388 (Fed. Cir. 1992). Although the specification may indicate that certain embodiments are preferred, particular embodiments appearing in the specification will not be read into the claims when the claim language is broader than the embodiments. *Electro Med. Sys., S.A. v. Cooper Life Sciences, Inc.*, 34 F.3d 1048, 1054 (Fed. Cir. 1994).

This Court's claim construction analysis is substantially guided by the Federal Circuit's decision in *Phillips v. AWH Corporation*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). In *Phillips*, the court set forth several guideposts that courts should follow when construing claims. In particular, the court reiterated that "the claims of a patent define the invention to which the patentee is entitled the right to exclude." 415 F.3d at 1312 (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). To that end, the words used in a claim are generally given their ordinary and customary meaning. *Id.* The ordinary and customary meaning of a claim term "is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Id.* at 1313. This principle of patent law flows naturally from the

recognition that inventors are usually persons who are skilled in the field of the invention and that patents are addressed to, and intended to be read by, others skilled in the particular art. *Id.*

Despite the importance of claim terms, *Phillips* made clear that "the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Id.* Although the claims themselves may provide guidance as to the meaning of particular terms, those terms are part of "a fully integrated written instrument." *Id.* at 1315 (quoting *Markman*, 52 F.3d at 978). Thus, the *Phillips* court emphasized the specification as being the primary basis for construing the claims. *Id.* at 1314-17. As the Supreme Court stated long ago, "in case of doubt or ambiguity it is proper in all cases to refer back to the descriptive portions of the specification to aid in solving the doubt or in ascertaining the true intent and meaning of the language employed in the claims." *Bates v. Coe*, 98 U.S. 31, 38 (1878). In addressing the role of the specification, the *Phillips* court quoted with approval its earlier observations from *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998):

> Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim. The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction.

Phillips, 415 F.3d at 1316. Consequently, *Phillips* emphasized the important role the specification plays in the claim construction process.

The prosecution history also continues to play an important role in claim interpretation. Like the specification, the prosecution history helps to demonstrate how the inventor and the Patent and Trademark Office ("PTO") understood the patent. *Id.* at 1317. Because the file

history, however, "represents an ongoing negotiation between the PTO and the applicant," it may lack the clarity of the specification and thus be less useful in claim construction proceedings. *Id.* Nevertheless, the prosecution history is intrinsic evidence that is relevant to the determination of how the inventor understood the invention and whether the inventor limited the invention during prosecution by narrowing the scope of the claims. *Id.*; *see Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1350 (Fed. Cir. 2004) (noting that "a patentee's statements during prosecution, whether relied on by the examiner or not, are relevant to claim interpretation").

Phillips rejected any claim construction approach that sacrificed the intrinsic record in favor of extrinsic evidence, such as dictionary definitions or expert testimony. The *en banc* court condemned the suggestion made by *Texas Digital Systems, Inc. v. Telegenix, Inc.*, 308 F.3d 1193 (Fed. Cir. 2002), that a court should discern the ordinary meaning of the claim terms (through dictionaries or otherwise) before resorting to the specification for certain limited purposes. *Phillips*, 415 F.3d at 1319-24. According to *Phillips*, reliance on dictionary definitions at the expense of the specification had the effect of "focus[ing] the inquiry on the abstract meaning of words rather than on the meaning of claim terms within the context of the patent." *Id.* at 1321. *Phillips* emphasized that the patent system is based on the proposition that the claims cover only the invented subject matter. *Id.*

Phillips does not preclude all uses of dictionaries in claim construction proceedings. Instead, the court assigned dictionaries a role subordinate to the intrinsic record. In doing so, the court emphasized that claim construction issues are not resolved by any magic formula. The court did not impose any particular sequence of steps for a court to follow when it considers disputed claim language. *Id.* at 1323-25. Rather, *Phillips* held that a court must attach the

appropriate weight to the intrinsic sources offered in support of a proposed claim construction, bearing in mind the general rule that the claims measure the scope of the patent grant.

In general, prior claim construction proceedings involving the same patents-in-suit are "entitled to reasoned deference under the broad principals of *stare decisis* and the goals articulated by the Supreme Court in *Markman*, even though *stare decisis* may not be applicable *per se*." *Maurice Mitchell Innovations, LP v. Intel Corp.*, No. 2:04-CV-450, 2006 WL 1751779, at *4 (E.D. Tex. June 21, 2006).

III. CONSTRUCTION OF AGREED TERMS

The Court hereby adopts the parties' agreement that in the Feldbau Patents, the term "set" means "group." (Dkt. No. 211, 11/29/2012 Joint Claim Construction and Prehearing Statement, at 5.) The Court also hereby adopts the parties' agreement that "terms that appear in both the preamble and the body of a claim serve as claim limitations." (*Id.*) The parties did not reach any other agreements prior to claim construction briefing.

IV. CONSTRUCTION OF DISPUTED TERMS IN THE "FELDBAU" PATENTS

For convenience, because the '219 Patent and the '334 Patent share a common specification, references to the specification shall be to the '219 Patent unless otherwise indicated.

The Abstracts of the Feldbau Patents are the same and state:

> Apparatus and method for authenticating that a sender has sent certain information via a dispatcher to a recipient is disclosed. The method includes the steps of: (a) providing a set A comprising a plurality of information elements a1, . . . an, said information element a1 comprising the contents of said dispatched information, and said one or more information elements a2, . . . an comprising dispatch-related information and compris[ing] at least the following elements: a2—a time indication associated with said dispatch; and a3—information describing the destination of said dispatch, and wherein at least one of said information elements is provided in a manner that is resistant or indicative of tamper attempts by said sender, (b) associating said dispatch-related information with said element a[1] by generating authentication-information, in particular

comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; (c) securing at least part of said authentication-information against undetected tamper attempts of at least said sender. The dispatch relates either to transmission or to manual delivery. The apparatus implements the operations of the method.

A. "authenticate the dispatch and the contents of the dispatch" ('219 Patent, Claim 60), "authenticating a dispatch and contents of the dispatch" ('219 Patent, Claims 60 and 71; '334 Patent, Claims 1 & 18), "authentication-information" ('219 Patent, Claim 30), and "authentication data" ('219 Patent, Claims 60 & 71; '334 Patent, Claims 1, 18 & 35)

"authenticate the dispatch and the contents of the dispatch" ('219 Patent, Claim 60) and "authenticating a dispatch and contents of the dispatch" ('219 Patent, Claims 60 and 71; '334 Patent, Claims 1 & 18)	
Plaintiffs' Proposal	**Defendants' Proposal**
"provide evidence capable of being used to prove the contents and dispatch"	Adobe proposes: "reliably determine the content of the sender's dispatch, the dispatch's destination, and the time the dispatcher sent the dispatch" (original claims) "reliably determine the content of the sender's dispatch, the dispatch's destination, and the time the recipient received the dispatch" (amended claims of '219 Patent) ReadNotify, RightSignature, Farmers, and Chris Drake propose: "the process of verifying and validating the content of the sender's dispatch, the dispatch's destination, and the time the dispatcher sent the dispatch" (original claims) "the process of verifying and validating the content of the sender's dispatch, the dispatch's destination, and the time the recipient received the dispatch" (amended claims of '219 Patent)

"authentication-information" ('219 Patent, Claim 30) and "authentication data" ('219 Patent, Claims 60 & 71; '334 Patent, Claims 1, 18 & 35)	
Plaintiffs' Proposal	**Defendants' Proposal**
"information that is associated with the contents of the dispatch by generating a representation of at least the elements a1, a2, and a3, the representation comprises one or more elements"	"information generated by an authenticator (such as a dispatcher)[5] that, in the event of a later dispute between sender and recipient, reliably allows a judge to determine what content was actually sent, a time related to when it was sent, and to where" (original claims) "data that allows one to reliably determine the content of the sender's dispatch, the dispatch's destination, and the time the recipient received the dispatch" (amended claims of '219 Patent)

(Dkt. No. 211, Ex. I, at 9-11; Dkt. No. 253, at 15; Dkt. No. 259, 1/31/2013 P.R. 4-5(d) Joint Claim Construction Chart, at 15 & 16-17.)

(1) The Parties' Positions

Plaintiffs argue that "[g]enerating the information 'authenticates' a message. In the lexicon of the '219 patent, merely having that evidence available supplies such 'authentication.' The later step of actually using and testing that information against another set of data is called 'verification.'" (Dkt. No. 251, at 7 (footnotes omitted).) Plaintiffs explain that authentication information cannot be used to reproduce the content of a dispatch and that verification is a separate, optional process. (*Id.*, at 7-8.) Plaintiffs urge that contrary to Defendants' arguments, the time of a recipient's receipt is not part of authentication and instead "concern[s] an optional and distinct aspect of the disclosed embodiments." (*Id.*, at 8.) Plaintiffs also argue claim differentiation as to dependent Claims 69, 79, and 88 of the '219 Patent. (*Id.*, at 9.)

[5] This parenthetical was omitted from Defendants' presentation slides at the February 14, 2013 hearing. (*See* Dkt. No. 271, Ex. A, at p. 12 of 90).

Defendants respond that "Plaintiffs would not require 'authentication information' to be useful for anything, to authenticate anything, or to prove anything." (Dkt. No. 253, at 16 (footnote omitted).) As to the "authenticate" and "authenticating" terms, Defendants respond that "[t]he core dispute is whether merely creating authentication evidence is enough to authenticate a dispatch and its contents (as Plaintiffs contend) or must that evidence be used to prove that the contents and dispatch are authentic (as Defendants contend)." (*Id.*)

Plaintiffs reply that their proposal for "authentication-information" is the construction that was reached in *Propat*. (Dkt. No. 257, at 4.) Plaintiffs also argue:

> No embodiment discloses information that, by itself, allows one to "reverse engineer" content and dispatch information. Instead, the embodiments process a purported set of data to test if its outputs match. The Defendants' construction that authentication-information alone may "reliably determine" the original data excludes all embodiments, and is wrong.

(*Id.*, at 5.) As to the remaining "authenticate" terms, Plaintiffs reiterate that "Defendants confuse 'authenticating' with 'verifying.'" (*Id.*) Plaintiffs note that "Claim 30's 'method for authenticating' stops at the point where the evidence is generated (the 'authentication-information'), and does nothing with it other than to secure it." (*Id.*)

At the February 14, 2013 hearing, Plaintiffs noted the following comment in a treatise that Defendants attached to their responsive brief: "In real life, adjudicators are seldom called. The inevitability of detection discourages cheating, and people remain honest." (Dkt. No. 253, Ex. B, Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* 24 (1993).) Plaintiffs thus argued that Defendants' own extrinsic evidence is consistent with Plaintiffs' proposal that authentication in the Feldbau Patents does not require actual verification.

(2) Analysis

As to "authentication-information," Plaintiffs propose substantially the same construction reached by the Central District of California in *Propat*: "authentication-information is information that is associated with the contents of the dispatch by generating a representation of at least the elements a1, a2, and a3, the representation comprises one or more elements, each comprising a representation of one or more elements of the set A." *Propat* at 3, 4 & 14.

Claim 1 of the '334 Patent recites (emphasis added):

> 1. A method of *authenticating a dispatch and contents of the dispatch* transmitted from a sender to a recipient, comprising the steps of:
>
> sending content data representative of the contents of the dispatch, and, a destination of the dispatch associated with said recipient, to an authenticator functioning as a non-interested third party with respect to the sender and the recipient, to be forwarded to said destination;
>
> receiving a representation of *authentication data* that has been generated by said authenticator, said *authentication data* comprising a representation of the following set A of information elements: a_1—comprising said content data, and dispatch record data elements $a_2, \ldots, a_n$ which includes at least an indicia a_2 relating to a time of the dispatch which is provided in a manner resistant to or indicative of tampering by either of the sender and the recipient, and an indicia a_3 relating to said destination of the dispatch,
>
> wherein at least part of said *authentication data* is secured against tampering of the sender and the recipient, and
>
> wherein said *authentication data* includes a set B comprising one or more information elements $b_1, \ldots, b_m$ generated by respectively applying functions $F_1, \ldots, F_m$ to subsets $S_1, \ldots, S_m$ comprising selected portions of said set A, where said functions $F_1, \ldots, F_m$ can be different from one another and said subsets $S_1, \ldots, S_m$ can be different from one another, and
>
> wherein said *authentication data* does not comprise an encrypted representation of said content data and said dispatch record data which is encrypted with a secret key, either symmetric or asymmetric, associated with said recipient.

Claim 1 of the '219 Patent recites (amendments by the Ex Parte Reexamination Certificate are shown with additions underlined and deletions in bolded square brackets; italics added for emphasis):

1. Apparatus for authenticating that certain information has been successfully transmitted from a sender via a dispatcher to a recipient, the apparatus comprising:

means for providing a set A comprising a plurality of information a1, . . . , an, where said information element a1 is originated from the sender and comprising the contents of the information being electronically transmitted to said recipient, and said one or more information elements a2, . . . , an comprising dispatch-related information and comprise at least the following elements:

a2—**[**a time indication associated with said dispatch**]** an indicia of a time of the successful transmission of the certain information to the recip[ie]nt, the indicia recorded by the dispatcher; and

a3—information describing the destination of said dispatch,

and wherein at least said information element a2 is provided in a manner that is resistant to or indicative of tampering by either of said sender and said recipient; and

an authenticator functioning as a non-interested third party with respect to the sender and the receiver and having

(1) means for associating said dispatch-related information with said element al by generating *authentication-information* comprising are [*sic*, a] representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and

(2) means for securing at least part of said *authentication-information* against tampering of said sender and recipient;

wherein at least one of the means for associating and for securing comprises means for generating a new set B, said set B comprising one or more information elements b1, . . . bm, each element bi comprising a representation of a subset Si, said representation being expressive as a function Fi of the elements of said subset Si, where said subset Si comprises a digital representation of at least one element of said set A, and where said functions Fi can be different.

The key dispute is whether "authenticating" and "authentication" relate to storing evidence of the dispatch and its content or, instead, require verification or validation of the dispatch and its content. The above-quoted claims do not recite verification or validation. Instead, authentication data is generated by the authenticator and secured against tampering. Likewise, the Summary of the Present Invention emphasizes the objective of providing "evidence" that "can" be used by the sender:

> It is therefore an object of the present invention to improve the capacity of conventional systems and methods for dispatching documents and transmitting

> information to *provide the sender with evidence he can use to prove both the dispatch and its contents*.

('219 Patent at 2:57-61 (emphasis added).) The specification further discloses:

> When it is desired to authenticate the dispatch of the original documents (and possibly also their receipt at the destination 30), either the sender or the document dispatching service provides the associated authentication-information, for example the envelope 32, unopened, to the party which required the authentication. When the envelope 32 is opened, it has associated therewith copies of both the dispatched documents and the dispatch information. The envelope 32 therefore, provides a *reliable proof that the original documents 12 were dispatched on the date and to the destination listed on or in envelope 32.*

(*Id.* at 5:63-6:6 (emphasis added).)

Finally, dependent Claims 69 and 79 of the '219 Patent (which depend from independent Claims 60 and 71, respectively), each recite "wherein the authentication data further includes a delivery indicia relating to said dispatch." The doctrine of claim differentiation therefore weighs in favor of finding that "authentication data" need not include an indication of delivery. *Phillips*, 415 F.3d at 1315 ("[T]he presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim.") (citing *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 910 (Fed. Cir. 2004)).

In sum, the claims and the specification are consistent with *Propat* and Plaintiffs' proposal. The Court accordingly hereby construes the disputed terms as set forth in the following chart:

Term	Construction
"authenticate the dispatch and the contents of the dispatch"	**"provide evidence capable of being used to prove the contents and the dispatch"**
"authenticating a dispatch and contents of the dispatch"	**"providing evidence capable of being used to prove the contents and the dispatch"**
"authentication-information" **"authentication data"**	**"information that is associated with the contents of the dispatch by generating a representation of at least the elements a1, a2, and a3, the representation comprising one or more elements"**

B. "dispatch" (All Claims), "contents of the dispatch" ('219 Patent, Claims 60 & 71), "content data" ('219 Patent, Claims 60 & 71; '334 Patent, Claims 1, 18 & 35), and "certain information" ('219 Patent, Claims 1 & 30)

"dispatch" (All Claims)	
Plaintiffs' Proposal	**Defendants' Proposal**
No need to construe; best to enter the jury instructions without explanation, with instruction that terms not specifically construed should be applied based on ordinary meaning to persons of skill in the art in the context of the intrinsic record. Alternatively: "the transmission sent from a sender to a recipient via a dispatcher"	Amazon, PayPal, DocuSign, Adobe, Zix, RightSignature, and Farmers propose: "the transmission sent from a sender toward a recipient via a dispatcher" ReadNotify and Chris Drake propose: "the act of transmission of the information being electronically transmitted from the sender to a recipient by a non-interested third party with respect to the sender and the receiver"
"contents of the dispatch" ('219 Patent, Claims 60 & 71) **"content data" ('219 Patent, Claims 60 & 71; '334 Patent, Claims 1, 18 & 35)**	
Plaintiffs' Proposal	**Defendants' Proposal**
"whatever information the sender originates for sending to the recipient"	"the entire content the sender originates for sending to the recipient"

"certain information" ('219 Patent, Claims 1 & 30)	
Plaintiffs' Proposal	**Defendants' Proposal**
Preamble not limiting[6] Alternatively: "whatever information the sender originates for sending to the recipient"	"the entire content the sender originates for sending to the recipient"

(Dkt. No. 211, Ex. I, at 4; Dkt. No. 259, 1/31/2013 P.R. 4-5(d) Joint Claim Construction Chart, at 13-14.)

(1) The Parties' Positions

Plaintiffs argue that the term "dispatch" is not limited to being a "message" and need not contain "destination information," which is recited elsewhere in the claims. (Dkt. No. 251, at 10.) As to the presence of an intermediary, Plaintiffs argue that "'dispatch' in its plain meaning is already known to be something relayed from a sender to a recipient through an intermediary." (*Id.*) Plaintiffs also argue that "requiring identity between the sent data and the received data [is] a notion foreign to the simple term 'dispatch.'" (*Id.*, at 11.) Finally, Plaintiffs submit that "dispatch" is used in the claims as a noun, not a verb. (*Id.*)

Defendants respond that "Defendants' construction limits the determination of the contents of the message to the sender, while Plaintiffs' construction would allow for the non-interested third party to determine the actual contents of the dispatch, so long as the dispatch

[6] The term "certain information" appears only in the preambles of original Claims 1 and 30 but also appears in the bodies of amended Claims 1 and 30. The parties have agreed that where a term appears in both the preamble and the body of a claim, the term is a limitation. (Dkt. No. 211, 11/29/2012 Joint Claim Construction and Prehearing Statement, at 5.) The parties briefing has not addressed whether "certain information" is a limitation in original Claims 1 and 30, so the Court does not address that issue.

includes something gleaned from the sender." (Dkt. No. 253, at 13-14.) Defendants reiterate that "no entity may act as both the sender and the non-interested third party dispatcher for a given transmission." (*Id.*, at 14 (footnote omitted).) Defendants further explain:

> Plaintiffs' construction implies that the non-interested third party need only forward "information" reflective of sender's message. But such a construction is diametrically opposed by the claims themselves. And, every embodiment in the specification features the sender creating the contents of the dispatch. There is no teaching where the third party dictates the content.

(*Id.*) Defendants conclude that "Plaintiffs' proposed constructions with respect to these terms would defeat the very purpose of the Feldbau techniques, which is to verify the contents of a message from a sender to a recipient, not to verify some modification or revision of that message made by the third party." (*Id.*, at 15 (footnote omitted).)

Plaintiffs reply:

> The claim language contradicts Defendants' contention that the "content" terms require that the third party cannot "'generate' or 'modify' or 'create' the information." Claim 30 recites that a1 merely "compris[es]" the contents of the information being electronically transmitted to the recipient. "Comprising" in patent claims is open ended. Claim 60 states that the content data is "representative of the contents of the dispatch," not that it is exactly identical to it. The same is true for claim 71.

(Dkt. No. 257, at 4 (footnote omitted).)

(2) Analysis

Claims 1 and 60 of the '219 Patent are representative and recite (amendments by the Ex Parte Reexamination Certificate are shown with additions underlined and deletions in bolded square brackets; italics added for emphasis):

> 1. Apparatus for authenticating that *certain information* has been successfully transmitted from a sender via a dispatcher to a recipient, the apparatus comprising:
>
> means for providing a set A comprising a plurality of information a1, . . . , an, where said information element a1 is originated from the sender and comprising the contents of the information being electronically transmitted to said

recipient, and said one or more information elements a2, . . . , an comprising dispatch-related information and comprise at least the following elements:

a2—**[**a time indication associated with said dispatch**]** an indicia of a time of the successful transmission of the *certain information* to the recip[ie]nt, the indicia recorded by the dispatcher; and

a3—information describing the destination of said *dispatch*,

and wherein at least said information element a2 is provided in a manner that is resistant to or indicative of tampering by either of said sender and said recipient; and

an authenticator functioning as a non-interested third party with respect to the sender and the receiver and having

(1) means for associating said dispatch-related information with said element al by generating authentication-information comprising are [*sic*, a] representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and

(2) means for securing at least part of said authentication-information against tampering of said sender and recipient;

wherein at least one of the means for associating and for securing comprises means for generating a new set B, said set B comprising one or more information elements b1, . . . bm, each element bi comprising a representation of a subset Si, said representation being expressive as a function Fi of the elements of said subset Si, where said subset Si comprises a digital representation of at least one element of said set A, and where said functions Fi can be different.

60. A method of authenticating a *dispatch* and *contents of the dispatch* successfully transmitted from a sender to a recipient, comprising the steps of:

receiving *content data* representative of the *contents of the dispatch* originated from the sender and being electrically transmitted to said recipient, and a destination of the *dispatch*;

providing an indicia **[**relating to**]** of a time of successful transmission of the *dispatch* to the recipient, said time related indicia being recorded by an authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient;

associating, by **[**an**]** the authenticator functioning as a non-interested third party with respect to the sender and the recipient, the *content data* with *dispatch* record data which includes at least said time related indicia and an indicia relating to the destination of the *dispatch*, to generate authentication data which authenticate the *dispatch* and the *contents of the dispatch*; and

securing, by said authenticator, at least part of the authentication data against tampering of the sender and the recipient;

wherein at least one of the steps of associating and securing utilizes mathematical association methods for a selected portion of a combination of the *content data* and the dispatched record data.

Although the specification does not define the term "dispatch," the Background of the Invention provides context:

> E-mail and other electronic message[] forwarding services are commonly used today. The sender sends a message to the dispatching service which, in turn, forwards the message to the destination and provides the sender with a delivery report which typically includes the date and time of the dispatch, the recipient's address, the transmission completion status, and sometimes even the transmitted data, the number of pages delivered, the recipient's identification information, and so on. The provided delivery report mainly serves for accounting purposes and for notifying the sender of the dispatch and/or its contents. Moreover, frequently no record of the specific dispatched data is maintained with the service after the delivery is completed or provided to the sender.

('219 Patent at 2:33-46.) The Summary of the Present Invention defines "contents of the dispatch" as "information" and provides further context for "dispatch":

> The term "the contents of the dispatch" herein refers to any information element having *information content* the substance of which is equivalent to that of the *information being dispatched*. This includes for example the information source, either in paper document or electronic form, the actual *dispatched information*, any copies thereof, any descriptive information or portion of the information contents identifying the dispatched information, and so forth regardless of the representation or form.
>
> * * *
>
> The *dispatch information* can be any information describing at least the time and destination of the dispatch and preferably the dispatch completion status. Other *information relating to the dispatch*, such as the identity of the sender and/or the recipient, handshake information, the actual elapsed dispatch time, the number of pages dispatched and so forth, the identification of the authenticator, for example its name, logo, stamp, etc., can also be provided.

(*Id.* at 4:8-16 & 4:30-37 (emphasis added).) The Detailed Description of the Preferred Embodiments also discloses, for example:

> When it is desired to authenticate the dispatch of the original documents (and possibly also their receipt at the destination 30), either the sender or the document dispatching service provides the associated authentication-information, for example the envelope 32, unopened, to the party which required the authentication. When the envelope 32 is opened, it has associated therewith copies of both the dispatched documents and the *dispatch information*. The

> envelope 32 therefore, provides a reliable proof that the original documents 12 were dispatched on the date and to the destination listed on or in envelope 32.
>
> * * *
>
> [I]ncorporation of identification information relating to the sender 701, the recipient 799 or both (either by means of their digital signature, or otherwise) in the certificate generated by the service 750, can provide for more complete authentication of the entire dispatch transaction, and can be used as evidence for the *dispatch and its contents* by both the sender and the recipient.

(*Id.* at 5:63-6:6 & 18:22-28.)

Although Plaintiffs propose that no construction is necessary for "dispatch," Plaintiffs' alternative proposal, which is substantially similar to the current proposal by most Defendants, would be helpful to the finder of fact. The proposal by ReadNotify and Chris Drake is rejected because "dispatch" is used in the claims to refer not to the act of transmission but rather to the thing being transmitted.

As to the remaining disputed terms, the parties agree that the "content" is something that "the sender originates for sending to the recipient," but the parties dispute whether those terms refer to "whatever information" or to "the entire content."

On balance, a person of ordinary skill in the art reading the Feldbau Patents as a whole would conclude that modification of the contents of a dispatch during transmission would be contrary to the claims and the specification. Instead, the "contents of the dispatch," for example, is conveyed from the sender to the recipient without modification. Defendants' proposed constructions should therefore be adopted. This finding does not, however, preclude the addition of other dispatch-related information, such as information related to routing, encryption, or authentication.

The Court hereby construes the disputed terms as set forth in the following chart:

Term	Construction
"dispatch"	**"the transmission sent from a sender toward a recipient via a dispatcher"**
"contents of the dispatch" **"content data"** **"certain information"**	**"the entire content the sender originates for sending to the recipient"**

C. "an indicia of a time of successful transmission of the dispatch to the recipient" ('219 Patent, Claim 30 (amended))

Plaintiffs' Proposal	Defendants' Proposal
"data representing a time associated with the transmission of the certain information from the dispatcher to the recipient"	Amazon, PayPal, Zix, DocuSign, ReadNotify, Chris Drake, RightSignature, and Farmers propose: "Data that proves both (a) the actual time at which the dispatch was delivered to the recipient, and (b) that the dispatch actually reached the recipient in a form the recipient was able to understand. This data must be obtained without any cooperation from the recipient." Adobe proposes: "data indicating the time the recipient received the dispatch"

(Dkt. No. 211, Ex. I, at 5; Dkt. No. 259, 1/31/2013 P.R. 4-5(d) Joint Claim Construction Chart, at 10-11; Dkt. No. 269, 2/13/2013 Joint Notice of Prioritized List of Claim Terms (Amazon, PayPal, and Zix adopted the proposal of DocuSign, ReadNotify, Chris Drake, RightSignature, and Farmers).)

(1) The Parties' Positions

Plaintiffs argue that "[t]he common mistake among all Defendants is misreading 'transmission' by the intermediary as 'receipt' or 'delivery' at the destination." (Dkt. No. 251, at 11.) Plaintiffs reiterate that "a 'successful transmission' is one that actually gets sent out from the dispatcher/authenticator toward the recipient, regardless of whether delivery ever occurs." (*Id.*, at 11-12.) Plaintiffs also argue claim differentiation as to dependent Claims 69, 79, and 88

of the '219 Patent. (*Id.*, at 12.) Plaintiffs conclude that "[w]hile the Feldbau patents do treat a successful transmission as a proxy for a successful delivery, that does not justify importing delivery-based limitations into a claim that explicitly uses the phrase 'successful transmission,' not 'successful delivery' or 'successful receipt.'" (*Id.* (footnote omitted).)

Defendants respond that during reexamination of the '219 Patent, "the patentee agreed to 'narrow the claimed indicia of time to be an indicia of a time of the successful transmission . . . of the dispatch,'" where "successful" transmission requires delivery to the recipient in readable form, proven without cooperation from the recipient. (Dkt. No. 253, at 4 (quoting Ex. E, 3/29/2012 Response After Final Office Action, at 10) (emphasis Defendants').) Defendants also argue that in distinguishing the "Bahreman" reference during reexamination, the patentee explained that in the patented invention, "only once the message is decrypted can there be a successful transmission." (*Id.*, at 5-6.) Finally, Defendants note Plaintiffs' acknowledgement in their opening brief that "the claims do not cover systems that require the recipient's cooperation to construct evidence of the *transmission*." (*Id.*, at 6 (citing Dkt. No. 251, at 9) (emphasis Plaintiffs').)

As to the relevant time, Defendants Amazon, PayPal, and Zix originally submitted that "the relevant time 'of' a transmission is when the dispatcher releases the message" because "[t]he specification includes an embodiment in which the non-interested third party preserves the time the message is released, and protects that time only after learning that the delivery was successful." (Dkt. No. 253, at 9.) As noted above, these Defendants have now joined in the proposal of DocuSign, ReadNotify, Chris Drake, RightSignature, and Farmers.

All Defendants now submit that the "'time of successful transmission' should be construed as the time that the dispatch was actually delivered to the recipient." (*Id.*) Defendants

focus on comments by the patentee during the reexamination of the '219 Patent, arguing that "the patentee clearly linked the concept of successful transmission with successful delivery." (*See id.*, at 8 (discussing Ex. E, 3/29/2012 Response After Final Office Action).)

All Defendants also argue that "Plaintiffs' construction reads out the word 'successfully' entirely" and "disavows explicit statements made before the Patent Office." (*Id.*, at 10.) Defendants argue that the embodiment cited by Plaintiffs, in which a "transmission completion" indication is "obtained from the communication protocol," encompasses unclaimed embodiments in which transmission fails and, regardless, does not support Plaintiffs' overbroad proposal of "a time *associated with* the transmission." (*Id.* (emphasis added).) Finally, Defendants argue that Plaintiffs' claim differentiation argument fails because delivery indicia have no bearing on the meaning of the time of "successful" transmission. (*Id.*, at 11.)

In reply, Plaintiffs cite column 7 of the specification and argue that "[a] claim covering 'transmitted' messages cannot cover untransmitted messages. RPost simply amended 'successful' into the claim language to make the USPTO's 'broadest reasonable interpretation' match what was already there." (Dkt. No. 257, at 1.) Plaintiffs emphasize that "the '219 patent contains no embodiment recording a 'time of receipt' at the recipient." (*Id.*) Plaintiffs argue that the embodiment in which a dispatch time is appended to a message "preferably after assuring that the message has been successfully delivered" is merely a "prefer[ed]" embodiment. (*Id.*, at 2.) Plaintiffs also argue that Defendants have taken portions of the reexamination out of context. (*Id.*) For example, "some reexamination comments that mention 'delivery' apply to those dependent claims" that "optionally call for a delivery indicia returning to the authenticator," "not the independent 'transmission' claims." (*Id.*) Plaintiffs also note that "the '219 patent sometimes equates mere 'transmissions' as a proxy for delivery." (*Id.*) Plaintiffs

further note that the "Herda" reference, considered during the original prosecution and during reexamination, used "delivery" to mean "the third party conveying the message outbound toward the recipient," which Plaintiffs submit "happens to be the same sense as 'transmission' by the third party in the '219 patent." (*Id.*, at 3.) Finally, Plaintiffs argue that the "Bahreman" and "Levine" references cited during reexamination "were different because their third party recorded a time it received the message, not a time it released it toward a recipient." (*Id.*)

At the February 14, 2013 hearing, Plaintiffs urged that the addition of the word "successful" did not change the scope of the claim because "successful" merely refers to successfully putting something on the communication network at the authenticator. Plaintiffs also submitted that there is no disclosed embodiment where a time stamp of the time of delivery comes back to the authenticator and becomes part of the authentication information.

Defendants responded that although "successful" does not require that the recipient actually open the message, the message must be delivered, in a readable form, and the proof of delivery must be obtained without cooperation of the recipient.

(2) Analysis

Claim 1 of the '219 Patent recites (amendments by the Ex Parte Reexamination Certificate are shown with additions underlined and deletions in bolded square brackets; italics added for emphasis):

> 1. Apparatus for authenticating that certain information has been *successfully* transmitted from a sender via a dispatcher to a recipient, the apparatus comprising:
>
> means for providing a set A comprising a plurality of information a1, . . . , an, where said information element a1 is originated from the sender and comprising the contents of the information being electronically transmitted to said recipient, and said one or more information elements a2, . . . , an comprising dispatch-related information and comprise at least the following elements:

a2—**[**a time indication associated with said dispatch**]** an indicia of a time of the *successful* transmission of the certain information to the recip[ie]nt, the indicia recorded by the dispatcher; and

a3—information describing the destination of said dispatch,

and wherein at least said information element a2 is provided in a manner that is resistant to or indicative of tampering by either of said sender and said recipient; and

an authenticator functioning as a non-interested third party with respect to the sender and the receiver and having

(1) means for associating said dispatch-related information with said element al by generating authentication-information comprising are [*sic,* a] representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and

(2) means for securing at least part of said authentication-information against tampering of said sender and recipient;

wherein at least one of the means for associating and for securing comprises means for generating a new set B, said set B comprising one or more information elements b1, . . . bm, each element bi comprising a representation of a subset Si, said representation being expressive as a function Fi of the elements of said subset Si, where said subset Si comprises a digital representation of at least one element of said set A, and where said functions Fi can be different.

The specification discloses:

> The service 750 forwards the message 701 to the recipient 799 using the address 704. The service 750, preferably after assuring that the message has been *successfully delivered,* adds (e.g., appends) a dispatch time indication 720 to the message 702 and the address 704, as well as information 708 indicating the *success (or failure) of the message delivery*. Obviously, additional dispatch information elements, such as a sequential dispatch number, the sender, recipient and the service identification information and so forth may be added as well.

('219 Patent at 16:2-12 (emphasis added).)

During reexamination of the '219 Patent, the patentee summarized examiner interviews in which the patentee explained the meaning of "successful" transmission:

> **A. Summary of Interview of February 15, 2012**
>
> RMail Limited, the owner of US. Patent No. 6,182,219 ("the '219 patent"), acknowledges the courtesies graciously extended by Examiners Andrew Nalven, Daniel Ryman and Henry Tran during the interview at the United States Patent and Trademark Office ("USPTO") on February 15, 2012. At the interview, Patent Owner was represent by Patent Owner's undersigned attorney, John K. Fitzgerald,

Dr. Terrence Tomkow (Patent Owner's Chief Technical Officer) and Zafar Khan (Patent Owner's Chief Executive Officer). Pursuant to 37 C.F.R. 1.560(b), Patent Owner provides the following summary of the interview.

During the interview, Dr. Tomkow provided an overview of the prior art references cited in the Final Office Action, that is, the Levine patent (US 3,393,566, the Bahreman reference (Certified Electronic Mail, Proceedings of the 1995 Network and Distributed Systems Security Conference, February 1994, pp. 3-19) and the Herda reference (Non-repudiation: Constituting evidence and proof in digital cooperation, Computers Standards & Interfaces 17 (1995) 69-79).

Dr. Tomkow also discussed the pending claims of the '219 patent in reference to the three prior art references, distinguishing those references from the pending claims. Patent Owner argued that the inventions of the '219 patent were not anticipated by the prior art references. *The '219 patent solves the problem of providing the sender of a message with evidence that a particular message had been received at a particular time even when the recipient denied receiving the message, disputed its content or disputed the time of delivery.* None of the prior art teaches or discloses the solution claimed in the '219 claims.

Dr. Tomkow and Patent Owner's representative further discussed *the necessity of construing the term "transmitted" as used in the preamble and body of the claims to mean that the transmission of a message from a sender to a recipient was successful; that is, that it meant that the message was successfully delivered to the recipient, or the recipient's agent,* even if the recipient denied receipt of the message.

Dr. Tomkow and Patent Owner's representative stated that the specification of the '219 patent shows that Feldbau (the inventor of the '219 patent) *always uses "transmits", "dispatches" and "sends" in the sense that entails <u>successfully</u> conveying a message to a recipient*. They pointed out moreover that Feldbau teaches methods whereby the dispatcher or authenticator would insure a transmission was successful. To ensure clarity of the claims, however, *Patent Owner agreed to amend the term transmission to state "successful transmission."* Other variations of the term "transmit" would be similarly amended.

The Examiners appeared to feel that the '219 claims were insufficiently clear in the way they described the data element (a2). In various independent claims, the element (a2) is recited as a time indicia or indication "relating to" or "associated with" the time of transmission. Even when "transmission" is explicitly constrained to successful transmissions, the Examiner stated that the terms "associated with" and "related to" were unacceptably vague. Patent owner agreed to amending the claims to make it clear that (a2) is indicative of the time of successful transmission, which is consistent with the specification of the '219 patent.

> As stated by Dr. Tomkow, *all of the prior art references rely upon a willing recipient*. That is, the third party, or dispatcher, or authenticator (hereinafter, collectively, "the dispatcher"[)], *only knows that the message has been successfully delivered to the recipient if the recipient tells the dispatcher that the recipient has received the message*.
>
> Dr. Tomkow and Patent Owner's representative pointed out that, in Levine and Bahreman[,] a trusted third party stamps a document, returns a copy to the sender and then attempts to send a copy to a recipient. *This does not provide any record that the document was received by the recipient. In contrast the claims of the '219 patent provide*[] *the sender with proof that a message was successfully sent to the recipient.*
>
> * * *
>
> **B. Summary of Interview of March 8, 2012**
>
> Patent Owner's attorney, John K. Fitzgerald, participated in a telephonic interview with Examiner Andrew Nalven on March 8, 2012. During the interview, Patent Owner's attorney proposed amending the independent claims of the '219 patent to narrow the claimed indicia of time to be an indicia of a time of the successful transmission of certain information (claims 1 and 30), and of the successful transmission of the dispatch (claim 60, 71 and 82), the indicia being recorded by the dispatcher (claims 1 and 30) or by the authenticator (claims 60, 71 and 82). The Examiner indicated that the proposed amendments would overcome the Herda, Levine and Bahreman references.

(Dkt. No. 253, Ex. E, 3/29/2012 Response After Final Office Action, at 7-8 & 10 (underlining in original; italics added).) In the same submission during reexamination, the patentee further emphasized "successful" transmission while distinguishing the Levine reference:

> Levine only provides a time stamp indicative of when the third party of Levine receives a message from a sender. Even if Levine is interpreted to provide a time stamp of when the message is sent from third party to the recipient, nowhere does Levine teach or suggest an indicia of a time of the successful transmission of the message to the recipient, because if Levine's third party sends the message on, *Levine captures no further information regarding whether the transmission was successful or not; at best, Levine can only prove the message was sent*. Further, there is nothing in Levine concerning recording an indicia of time of the successful transmission by an authenticator.
>
> In contrast, Levine describes a form of electronic Notary service in which a document is time stamped by a third party en route from a first party to a second party. The time stamp applied by Levine is indicative of the time at which the

> third party receives the document. It proves that that document, with its specific content, existed at a certain time. It *does not prove the document was ever delivered* to the second party. If the document *cannot be transmitted*, due to some *error of transmission or even if it is misaddressed*, this will make no difference to the time indicia applied according to Levine's method. Levine's time stamp is not therefore "an indicia of the time of successful transmission of the dispatch to the recipient."
>
> * * *
>
> [A]ll of these time stamping steps [in Levine] record the time the document is received by Levine's system and not when (if ever) the message is *successfully transmitted to a recipient*. Nowhere does Levine teach or suggest recording the time at which the document is *successfully forwarded* from his Notary service to the recipient. In fact, the most Levine says about sending a time-stamped document on to a receiver is that the document is placed in a queue for possible transmission at a later time. See, Levine, Col. 6, ll. 53-64. Nothing in his method is responsive to, nor does Levine take notice of, the possibility that the transmission might fail or never occur.
>
> * * *
>
> Additionally, Levine does not render amended claim 71 obvious because *Levine makes no provision for the possibility that a message might fail to reach a recipient*. One skilled in the art would not develop a system based on the teachings of Levine that would provide a means for providing an indicia of a time of successful transmission of the dispatch to a receiving system, the time indication being recorded by the authenticator[,] without significant further development of the concepts disclosed by Levine.

(*Id.*, at 14-15, 16 & 19 (emphasis added).)

The patentee's arguments distinguishing the "Bahreman" reference during reexamination of the '219 Patent provide further context for "successful transmission":

> Claims 1-26, 29-56, 58-64, 66-76, 78-84 and 86-89 were rejected under 35 U.S.C. 102(b) as being anticipated by Bahreman. Patent Owner traverses these rejections and, in view of the arguments presented below, requests that the rejections be withdrawn and a timely certificate of patentability be issued.
>
> 1. Claim 1
>
> (a) Amended claim 1 is not anticipated by Bahreman because Bahreman fails to disclose an indicia of a time of

> the successful transmission of certain information to a recipient, the indicia recorded by a dispatcher
>
> Claim 1 was amended to recite an element a2 where a2 is an indicia of a time of the successful transmission of certain information to the recipient, the indicia recorded by the dispatcher. Bahreman fails to disclose or even suggest such an indicia.
>
> Bahreman only teaches keeping a record of the time of receipt of the message by the TTP (trusted third party) from the sender. *Nowhere does Bahreman teach or even suggest obtaining an indicia of time of the successful transmission* of the information, nor does Bahreman disclose recording such an indicia. Bahreman does teach receiving a request from Rob for the key to open the ciphertext he received from TTP, and teaches the TTP sending the key to Rob, but nothing in this exchange discloses anything regarding an indicia of a time of a successful transmission of the message because *the transmission is only successful in Bahreman's system if the key received by Rob from the TTP actually opens the message. Moreover, because Bahreman does not disclose any communication between Rob and TTP as occurring after the key is sent to Rob, there is no way that TTP can record an indicia of time of successful transmission of the message to Rob.*
>
> * * *
>
> [A] *proof of mailing is not the same thing as proof of successful transmission of the message for the simple reason that the message may be mailed but never delivered.*

(*Id.*, at 20 & 21 (emphasis added).)

> The patentee made a similar statement in the ongoing reexamination of the '334 Patent:
>
> The '334 Patent addresses this problem in the "Summary" section, stating: "The literature does not provide a comprehensive solution that directly addresses the problem in question: "what information has been sent to whom and when." Summary, Col. 2, ll. 51-54. The concept of a *successful transmission meaning that the message or dispatch actually got to the recipient (even if the recipient denies receiving the message or dispatch)* is also supported by the statement "The dispatch information can be any information describing at least the time and destination of the dispatch <u>and preferably the dispatch completion status</u>." *Id.* at Col. 4, ll. 33-35 (emphasis added).

(Dkt. No. 253, Ex. I, 3/13/2012 Supplemental Response to Non-Final Office Action, at 9

(underlining in original; italics added); *Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d

1295, 1306 (Fed. Cir. 2007) ("[A] statement made by the patentee during prosecution history of a patent in the same family as the patent-in-suit can operate as a disclaimer.") (citing *Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1350 (Fed. Cir. 2004)).)

On balance, the above-quoted passages constitute "definitive statements" by the patentee that: (1) the success of the transmission is determined without cooperation of the recipient; and (2) "successful" transmission requires that the dispatch reaches a point at which it becomes available for receipt by the recipient. *Schindler Elevator Corp. v. Otis Elevator Co.*, 593 F.3d 1275, 1285 (Fed. Cir. 2010) (noting that a patent owner "is not entitled to any interpretation that is disclaimed during prosecution"); *Omega Eng. v. Raytek Corp.*, 334 F.3d 1314, 1324 (Fed. Cir. 2003) ("As a basic principle of claim interpretation, prosecution disclaimer promotes the public notice function of the intrinsic evidence and protects the public's reliance on *definitive* statements made during prosecution.") (emphasis added). Stated another way, "successful" transmission requires that the sender, and any intermediate parties acting upon the sender's request to transmit the dispatch, have accomplished all that is normally within their control to put the dispatch in a place where the recipient may later be able to retrieve the dispatch. The determination of this success is accomplished without any cooperation by the recipient, and whether the recipient ever actually retrieves the dispatch is irrelevant to "successful transmission."

Nonetheless, although the above-quoted prosecution history refers to the time of delivery, no "definite" statement is evident that requires interpreting the phrase "time of the successful *transmission*" to refer to the time of successful *delivery*. Instead, because the claims recite "transmission" rather than "receipt" or "delivery," the better reading is that the relevant time is when the dispatch was released from the control of the non-interested third party. Further,

dependent Claims 69 and 79 of the '219 Patent recite "wherein the authentication data further includes a delivery indicia relating to said dispatch." This distinction between "transmission" and "delivery," as used in the claims, provides additional support for interpreting the time of "successful transmission" to mean the time of release of the dispatch from the non-interested third party rather than the time of delivery to the recipient. Presumably, then, the time of delivery is later than the time of transmission.

As to Defendants' proposal that "the dispatch actually reached the recipient in a form the recipient was able to understand," the prosecution history is not definitive. While distinguishing the Bahreman reference, the patentee noted that "the transmission is only successful in Bahreman's system if the key received by Rob from the TTP actually opens the message." (Dkt. No. 253, Ex. E, 3/29/2012 Response After Final Office Action, at 20 & 21.) On balance, this does not amount to a "definitive statement" that a "successful transmission" in the '219 Patent requires that the "the recipient was able to understand" the dispatch. *Omega Eng.*, 334 F.3d at 1324 ("As a basic principle of claim interpretation, prosecution disclaimer promotes the public notice function of the intrinsic evidence and protects the public's reliance on *definitive* statements made during prosecution.") (emphasis added).

Finally, as to Defendants' proposal that the data must "prove" the time at which a dispatch was forwarded, the term "prove" might be read too narrowly by the finder of fact as requiring absolute proof. Instead, as proposed by Plaintiffs, the data need only "represent" the time. Likewise, the meaning of Defendants' proposal of "actual time" rather than simply "time" is unclear and potentially too narrow.

The Court therefore hereby construes **"an indicia of a time of successful transmission of the dispatch to the recipient"** to mean **"data that represents the time at which the**

dispatcher forwarded the dispatch for delivery such that the recipient may later be able to receive the dispatch and where the data is obtained without any cooperation from the recipient."

D. "an indicia relating to a time of transmission of the dispatch" ('219 Patent, Claims 60 & 71 (original)) and "an indicia a2 relating to a time of the dispatch" ('334 Patent, Claims 1, 18 & 35)

Plaintiffs' Proposal	**Defendants' Proposal**
"data representing a time associated with the transmission of the certain information from the authenticator / dispatcher to the recipient"	"data showing a time that is related in some way to the specific time a dispatch was sent to someone"

(Dkt. No. 211, Ex. I, at 6; Dkt. No. 253, at 11 (Defendants have agreed upon one jointly proposed construction); *see* Dkt. No. 259, 1/31/2013 P.R. 4-5(d) Joint Claim Construction Chart, at 8, 10 & 19.)

(1) The Parties' Positions

Plaintiffs' opening brief does not address these terms apart from the similar term "an indicia of a time of successful transmission of the dispatch to the recipient." (*See* Dkt. No. 251.)

Defendants argue that "[a]ll Defendants agree that this 'a2' need not indicate a successful transmission, and even Plaintiffs agree this language is not limited to either time of release or time of delivery." (Dkt. No. 253, at 11.)

Plaintiffs reply that "Plaintiffs do not 'agree that this language is not limited to either time of release or time of delivery.' Indeed, it means the same thing that the pre- and post-amendment a2 terms mean from the '219 patent—the time of the outbound transmission of the message from the third party toward the recipient." (Dkt. No. 257, at 3.)

At the February 14, 2013 hearing, Defendants submitted that to aid clarity, Defendants' proposal of the words "specific" and "to someone" could be omitted from the construction.

(2) Analysis

Unlike the similar term "an indicia of a time of successful transmission of the dispatch to the recipient," the present disputed terms do not require a "successful" transmission. Also, Plaintiffs have not shown why the general language "time of transmission of the dispatch" should be limited to the time a dispatch is sent "from the authenticator / dispatcher to the recipient." In other words, Plaintiffs have failed to demonstrate that the time "relating to a time of transmission" cannot be the time of delivery. As to Defendants' proposal, however, Defendants have failed to demonstrate the necessity of a "specific" time.

The Court therefore hereby substantially adopts Defendants' proposal but modifies it so as to construe **"an indicia relating to a time of transmission of the dispatch"** and **"an indicia a2 relating to a time of the dispatch"** to mean **"data showing a time that is related to the time a dispatch was sent."**

E. "resistant to or indicative of tampering by either of the sender and the recipient" (All Claims)

Plaintiffs' Proposal	**Defendants' Proposal**
"treated in a way that makes tampering by the sender or recipient difficult or easily detected, including non-limiting examples of placing in secure storage, subjecting to mathematical association methods, or both"	"treated in a way that makes the data unalterable, or that makes unauthorized alteration detectable, such that the original data cannot be disputed"

(Dkt. No. 211, Ex. I, at 17; Dkt. No. 253, at 17; Dkt. No. 259, 1/31/2013 P.R. 4-5(d) Joint Claim Construction Chart, at 18.)

(1) The Parties' Positions

Plaintiffs argue that "'[r]esistant to . . . tampering' means it is 'difficult' to tamper" and that "'[i]ndicative of tampering' means that tampering is detectable." (Dkt. No. 251, at 12.) Plaintiffs submit that Defendants' proposal either "simply refers back to a prior disputed term" or "omits any expression of what the term itself might mean (much less any mechanism for achieving the goal)." (*Id.*)

Defendants respond that "the ['219] patent consistently and repeatedly refers to the indisputable nature of the information by calling it 'proof,' 'reliable proof,' 'evidence,' and noting it could be used in 'a court of law.'" (Dkt. No. 253, at 18 (citing '219 Patent at 2:57-65, 4:19-29 & 6:15-16).) Defendants also cite arguments by the patentee during reexamination that the '219 Patent provides proof in case the recipient disputes delivery. (*Id.* (citing Ex. E, 3/29/2012 Response After Final Office Action, at 7).) Finally, Defendants argue that Plaintiffs' proposed construction relies upon attorney argument rather than any evidence. (*Id.*, at 18-19.)

Plaintiffs reply that the disputed term is readily understandable and that "the fact an invention meets several objectives does not limit the claim to structures that achieve all of the objectives." (Dkt. No. 257, at 6.)

(2) Analysis

On balance, references to "proof," "reliable proof," "evidence," and that information could be used in "a court of law" ('219 Patent at 2:57-65, 4:19-29 & 6:15-16) are insufficient to require "that the data cannot be disputed." To the extent the patents-in-suit use a "court of law" as an example (*id.* at 6:15-16), this Court is well aware that proof and evidence are rarely beyond dispute. Defendants' proposed construction is therefore expressly rejected.

Plaintiffs' proposal, however, adds little to the plain language of the disputed term except to add the "nonlimiting" examples of "placing in secure storage, subjecting to mathematical association methods, or both." These examples are unnecessary and are expressly rejected.

The Court therefore hereby construes **"resistant to or indicative of tampering by either of the sender and the recipient"** to have its **plain meaning**. The Court hereby expressly rejects Plaintiffs' proposed examples as well as Defendants' proposal to require "that the data cannot be disputed."

F. "authenticator" (All Claims)

Plaintiffs' Proposal	**Defendants' Proposal**
"a digital electronic subsystem that operates to authenticate a dispatch and functions as a noninterested third party with respect to the sender and the recipient"	"a sub-system that generates authentication data for a dispatch"

(Dkt. No. 211, Ex. I, at 12; Dkt. No. 253, at 17.)

(1) The Parties' Positions

Plaintiffs argue that they propose the prior construction reached by the Central District of California in *Propat*, except Plaintiffs propose including that the subsystem is "digital electronic" because:

> (1) the human-only embodiment of the ideas of the '219 patent did not use the term "authenticator," and was not claimed; (2) the electronic-only embodiments do use the term "authenticator;" (3) the broadest usage of the term "authenticator" denotes an "apparatus" that is "constructed" and is "electronic;" (4) the originally-filed claims did not have "authenticator" language because that was added later by amendment; and (5) other amendments confirmed that the electronic information that the authenticator operated upon was "data," connoting something "digital."

(Dkt. No. 251, at 13.) Plaintiffs argue that Defendants' proposal that "the 'authenticator' is the subsystem that 'generates' the authentication-information, and does so without sender/recipient cooperation, . . . is already implicit in [Plaintiffs'] construction." (*Id.*)

Defendants respond that "Plaintiffs' proposal is nearly identical [to Defendants], but errs in limiting the term to electronic communications, when the specification includes examples of non-electronic communications as well." (Dkt. No. 253, at 17.)

Plaintiffs reply that "Defendants' cites to the specification do not use the word 'authenticator.' All specification uses of the word 'authenticator' refer to an electronic apparatus." (Dkt. No. 257, at 5.)

(2) Analysis

Propat construed "authenticator" to mean "a sub-system that operates to authenticate a dispatch and functions as a non-interested third party with respect to the sender and the recipient." *Propat* at 4, 7 & 14. As a threshold matter, all parties in the above-captioned case agree that an "authenticator" is a "sub-system" of some kind.

In *Propat,* the parties agreed that the construction should include "functions as a non-interested third party with respect to the sender and the recipient." (*See id.* at 4.) Here, only Plaintiffs' proposal includes such language. On balance, that language should be omitted because it is redundant in, for example, Claim 1 of the '219 Patent, which recites "an authenticator functioning as a non-interested third party with respect to the sender and the receiver."

As to whether the authenticator must be "digital electronic," as Plaintiffs propose, Claim 1 of the '334 Patent is representative and recites (emphasis added):

> 1. A method of authenticating a dispatch and contents of the dispatch transmitted from a sender to a recipient, comprising the steps of:
>
> sending content data representative of the contents of the dispatch, and, a destination of the dispatch associated with said recipient, to an *authenticator* functioning as a non-interested third party with respect to the sender and the recipient, to be forwarded to said destination;
>
> receiving a representation of authentication data that has been generated by said *authenticator*, said authentication data comprising a representation of the

> following set A of information elements: a_1—comprising said content data, and dispatch record data elements $a_2, \ldots, a_n$ which includes at least an indicia a_2 relating to a time of the dispatch which is provided in a manner resistant to or indicative of tampering by either of the sender and the recipient, and an indicia a_3 relating to said destination of the dispatch,
>
> wherein at least part of said authentication data is secured against tampering of the sender and the recipient, and
>
> wherein said authentication data includes a set B comprising one or more information elements $b_1, \ldots, b_m$ generated by respectively applying functions $F_1, \ldots, F_m$ to subsets $S_1, \ldots, S_m$ comprising selected portions of said set A, where said functions $F_1, \ldots, F_m$ can be different from one another and said subsets $S_1, \ldots, S_m$ can be different from one another, and
>
> wherein said authentication data does not comprise an encrypted representation of said content data and said dispatch record data which is encrypted with a secret key, either symmetric or asymmetric, associated with said recipient.

Nothing in Claim 1 of the '334 Patent suggests or implies that the "authenticator" must be electronic. Thus, the generic term "authenticator," by itself, is not limited to a digital electronic system. Further, the specification explains that the invention encompasses both electronic and non-electronic communication:

> The present invention encompasses all types of information being dispatched, such as that found *on paper documents or within electronic documents* and other electronic data, and *all types of dispatch methods*, such as transmission via facsimile machines, modems, computer networks, *electronic* mail systems and so forth, or *manually* such as via registered mail or courier services.
>
> * * *
>
> Reference is now made to FIG. 1 which illustrates *the method of the present invention as it can be implemented for paper documents being sent non-electronically.* The method of FIG. 1 can be implemented for documents sent via any document dispatching service, such as a courier service or the registered mail service of the post office.

('219 Patent at 4:1-7 & 4:66-5:4 (emphasis added).)

The Court therefore substantially adopts the *Propat* construction, with the exception of the "non-interested" phrase, as noted above, and hereby construes **"authenticator"** to mean **"a sub-system that operates to authenticate a dispatch."**

G. "sender," "recipient," and "non-interested third party" (All Claims)

"sender" (All Claims)	
Plaintiffs' Proposal	**Defendants' Proposal**
No need to construe; best to enter the jury instructions without explanation, with instruction that terms not specifically construed should be applied based on ordinary meaning to persons of skill in the art in the context of the intrinsic record. Alternatively: "an entity or device that sends content to a recipient"	"the party who determines the content of a dispatch and identifies its intended destination"
"recipient" (All Claims)	
Plaintiffs' Proposal	**Defendants' Proposal**
No need to construe; best to enter the jury instructions without explanation, with instruction that terms not specifically construed should be applied based on ordinary meaning to persons of skill in the art in the context of the intrinsic record. Alternatively: "an entity or device that receives content from a sender"	"the party to whom the sender's dispatch is directed"
"non-interested third party" (All Claims)	
Plaintiffs' Proposal	**Defendants' Proposal**
No need to construe; best to enter the jury instructions without explanation, with instruction that terms not specifically construed should be applied based on ordinary meaning to persons of skill in the art in the context of the intrinsic record. RPost also objects to construing this partial term[, which] should not be construed apart from the full term in which it exists.	"a third party who carries out the authentication function without the cooperation of the sender or the recipient, and who has no interest in the dispatch"

Alternatively: "a party who would carry out the authentication function without bias and without the participation of the sender or the recipient"	

(Dkt. No. 211, Ex. I, at 1 & 2; Dkt. No. 259, 1/31/2013 P.R. 4-5(d) Joint Claim Construction Chart, at 11-13.)

(1) The Parties' Positions

Plaintiffs submit that their proposal accords with the analysis of the Central District of California in *Propat*. (Dkt. No. 251, at 14.) Plaintiffs argue that Defendants' proposal to replace "without the participation" with "without the cooperation" "detracts unnecessarily from the clarity of the earlier construction." (*Id.*) Similarly, Plaintiffs argue that Defendants' proposal to replace "unbiased . . . in carrying out the operations of the authenticator" with "no interest in the dispatch" is unclear, and Plaintiffs are "concerned that any entity that has a profit motive will, in some fashion, have an 'interest' in the transactions it processes" under Defendants' proposed interpretation. (*Id.*, at 14-15.)

Defendants respond that the claims define "sender," "recipient," and "non-interested third party" as "distinct entities with distinct functions." (Dkt. No. 253, at 12.) Defendants also cite prosecution history in which, according to Defendants, "the patent owner made clear that a party who composes a document using information gleaned from others—as a Certificate Authority uses a customer's public key in creating a certificate—'is actually the 'sender' in [that process] and cannot be both a sender and an independent, non-interested, third party at the same time.'" (*Id.* (citing Ex. K, 2/3/2000 Remarks in Amendment, at 18).) Finally, Defendants urge that "'non-interested' necessarily implies that the third party has no input; it has no interest in the content." (*Id.*, at 13.)

Plaintiffs reply that "[i]f any explanation is required, the 'sender' may be named 'the entity or system who originates a message.'" (Dkt. No. 257, at 4.) As to "non-interested," Plaintiffs cite the *Propat* decision, where "the California court cited the intrinsic record to show that the authentication function is performed 'without bias.'" (*Id.*)

(2) Analysis

As a threshold matter, the disputed terms "sender" and "recipient" are readily understandable, and Defendants have not demonstrated any special meaning or any substantive dispute that requires resolution by the Court. The Court therefore hereby expressly rejects Defendants' proposed constructions for "sender" and "recipient" and instead adopts Plaintiffs' proposal that no construction is required.

Propat construed "functioning as a non-interested third party with respect to the sender and the recipient" to mean "the authenticator functions like an unbiased party would function with respect to the sender and the receiver, in carrying out the operations of the authenticator, and carries out its authentication function without the participation of the sender or the recipient." *Propat* at 10 & 14.

The parties dispute whether the non-interested third party "has no interest" or merely operates "without bias" and whether the non-interested third party operates without "cooperation" of the sender or recipient or without "participation" of the sender or recipient.

On balance, the Court agrees with Plaintiffs that Defendants' proposals of "without the cooperation" and "no interest in the dispatch" are not supported by the intrinsic evidence and would tend to confuse rather than clarify. In particular, Defendants' proposal of "no interest in the dispatch" might be read to exclude an entity that collects a fee for processing the dispatch.

The Court therefore hereby construes the disputed terms as set forth in the following chart:

Term	Construction
"sender"	**Plain meaning**
"recipient"	**Plain meaning**
"non-interested third party"	**"a party who carries out the authentication function without bias and without the participation of the sender or the recipient"**

H. "means for providing an indicia relating to a time of transmission of the dispatch . . ." ('219 Patent, Claim 71)

"means for providing an indicia relating to a time of transmission of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient" ('219 Patent, Claim 71 (original))	
Plaintiffs' Proposal	**Defendants' Proposal**
The function of this limitation is providing an indicia of a time the dispatch was successfully transmitted to the destination receiving system. The corresponding structures disclosed in the specification are an internal clock 50 located within the authenticator or an externally obtained time source that is secured from being set by an interested party such as the sender.	Amazon, PayPal, DocuSign, ReadNotify, and Chris Drake propose: This language triggers Sec. 112, ¶ 6. Function: providing sender with "an indicia relating to a time of transmission of the dispatch," said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient. The function needs no separate construction. Structure: The structure includes non-electronic embodiments, such as Fig. 1 (item 16) and 219.5:5-6:30[;] Fig 1 (item 16) and 219.5:5-6:30 (nonelectronic embodiment); Fig. 2 (item 66) and 219.7:12-28; Fig. 3 (item 66); Fig. 4 ("TIME INDICATION" arrow) and 219.13:8-18; Fig. 7 (time indication 720) and 219 13:11-16, 16:3-32, 16:60-17:13, 17:59-18:22. Adobe proposes: Subject to § 112, ¶ 6. Function: providing an indicia relating to a time of transmission of the dispatch, said time related indicia being provided in a manner resistant to or indicative of

	tampering by either of the sender and the recipient Structure: A secure clock internal to the authenticator or a clock external to the authenticator that is secured from being set or modified by an interested party such as the sender.
"means for providing an indicia of a time of successful transmission of the dispatch to the receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient" ('219 Patent, Claim 71 (amended))	
Plaintiffs' Proposal	**Defendants' Proposal**
The function of this limitation is providing an indicia of a time the dispatch was successfully transmitted to the destination receiving system. The corresponding structures disclosed in the specification are an internal clock 50 located within the authenticator or an externally obtained time source that is secured from being set by an interested party such as the sender.	This language triggers Sec. 112, ¶ 6. Function: providing "an indicia of a time of successful transmission of the dispatch to the receiving system," said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient. The success of the transmission is determined without the cooperation of the recipient. ("Tampering" means to alter in an unauthorized way.) Structure: No corresponding structure for performing this function is disclosed in the patent or linked to this function in the intrinsic evidence.

(Dkt. No. 211, Ex. I, at 7-8; Dkt. No. 259, 1/31/2013 P.R 4-5(d) Joint Claim Construction Chart, at 32-35.) Defendants thus present different proposals for the term in original Claim 71 as opposed to the term as amended by the Reexamination Certificate.

(1) The Parties' Positions

Plaintiffs argue that the corresponding structures, namely "internal clock 50" or, alternatively, an "externally obtained time indication 66," are explicitly disclosed in the specification. (Dkt. No. 251, at 16 (citing '219 Patent at col. 7).)

As to amended Claim 71, which recites "a time of *successful* transmission," Defendants respond that "[t]he function is not providing the current time. Rather, . . . the function is providing an indication that a transmission was released or delivered at a particular time and that

it actually reached its destination in a readable form and providing that confirmation without cooperation of the recipient." (Dkt. No. 253, at 19.) Defendants argue that "the only support in the specification for obtaining confirmation of successful delivery to the recipient requires the recipient to cooperate by providing a countersignature," which Defendants argue "provides no support for achieving this same end without any such cooperation." (*Id.*) Defendants conclude that "the patent lacks the required disclosure of corresponding structure for this claimed function." (*Id.*)

Plaintiffs reply that in the specification, a "time indication for the transmission" is provided by the internal clock in a dispatcher. (Dkt. No. 257, at 6 (citing '219 Patent at 7:13-14).)

(2) Analysis

Indefiniteness is a "legal conclusion that is drawn from the court's performance of its duty as the construer of patent claims." *Exxon Research & Eng'g Co. v. U.S.*, 265 F.3d 1371, 1376 (Fed. Cir. 2001) (citation omitted). A finding of indefiniteness must overcome the statutory presumption of validity. *See* 35 U.S.C. § 282. That is, the "standard [for finding indefiniteness] is met where an accused infringer shows by clear and convincing evidence that a skilled artisan could not discern the boundaries of the claim based on the claim language, the specification, and the prosecution history, as well as her knowledge of the relevant art area." *Halliburton Energy Servs., Inc. v. M-I LLC*, 514 F.3d 1244, 1249-50 (Fed. Cir. 2008).

> In determining whether that standard is met, i.e., whether the claims at issue are sufficiently precise to permit a potential competitor to determine whether or not he is infringing, we have not held that a claim is indefinite merely because it poses a difficult issue of claim construction. We engage in claim construction every day, and cases frequently present close questions of claim construction on which expert witnesses, trial courts, and even the judges of this court may disagree. Under a broad concept of indefiniteness, all but the clearest claim construction issues could be regarded as giving rise to invalidating indefiniteness

> in the claims at issue. But we have not adopted that approach to the law of indefiniteness. We have not insisted that claims be plain on their face in order to avoid condemnation for indefiniteness; rather, what we have asked is that the claims be amenable to construction, however difficult that task may be. If a claim is insolubly ambiguous, and no narrowing construction can properly be adopted, we have held the claim indefinite. If the meaning of the claim is discernible, even though the task may be formidable and the conclusion may be one over which reasonable persons will disagree, we have held the claim sufficiently clear to avoid invalidity on indefiniteness grounds. . . . By finding claims indefinite only if reasonable efforts at claim construction prove futile, we accord respect to the statutory presumption of patent validity . . . and we protect the inventive contribution of patentees, even when the drafting of their patents has been less than ideal.

Exxon, 265 F.3d at 1375 (citations and internal quotation marks omitted).

Title 35 U.S.C. § 112 ¶ 6, allows a patentee to express a claim limitation as "a means or step for performing a specified function without the recital of structure, material, or acts in support thereof." *See Inventio AG v. Thyssenkrupp Elevator Ams.*, 649 F.3d 1350, 1355-56 (Fed. Cir. 2011). The Federal Circuit has further clarified what such functional claiming requires:

> Thus, in return for generic claiming ability, the applicant must indicate in the specification what structure constitutes the means. If the specification is not clear as to the structure that the patentee intends to correspond to the claimed function, then the patentee has not paid the price but is rather attempting to claim in functional terms unbounded by any reference to structure in the specification. Thus, if an applicant fails to set forth an adequate disclosure, the applicant has in effect failed to particularly point out and distinctly claim the invention as required by the second paragraph of § 112.

Biomedino, LLC v. Waters Techs. Corp., 490 F.3d 946, 948 (Fed. Cir. 2007) (citations and internal quotation marks omitted). "Although one of skill in the art may have been able to find a structure that would work, that does not satisfy § 112 ¶ 6. Under § 112 ¶ 6, a patentee is only entitled to 'corresponding structure . . . described in the specification and equivalents thereof,' not any device capable of performing the function." *Ergo Licensing, LLC v. Carefusion 303, Inc.*, 673 F.3d 1361, 1364 (Fed. Cir. 2012) (citing *Blackboard, Inc. v. Desire2Learn Inc.*, 574 F.3d 1371, 1385 (Fed. Cir. 2009)) (emphasis in original).

"[T]he written description must clearly link or associate structure to the claimed function." *Telcordia Techs., Inc. v. Cisco Sys., Inc.*, 612 F.3d 1365, 1376 (Fed. Cir. 2010). Failure to disclose adequate structure corresponding to the claimed function results in the claim being invalid for indefiniteness. *See, e.g., Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1338 (Fed. Cir. 2008).

The specification discloses:

> The *internal clock 50* provides an indication 66 of the current time, and is utilized to provide a time indication for the transmission. *Internal clock 50* is securable (to ensure the veracity of the produced *time indication 66*), and preferably provides time indications according to a non-changing time standard, such as Greenwich-Mean-Time (G.M.T.) or UTC.[7] Alternatively, the *time indication 66 can be externally obtained, for example from a communication network server*, as long as the source is secured from being set or modified by an interested party such as the sender. The security of the time indication can be provided in a number of ways, such as by factory pre-setting the *clock 50* and disabling or password securing the Set Date/Time function of the *internal clock 50*. Alternatively, the *clock 50* can maintain a "true offset" with the true preset date/time, that reflects the offset of the user set date/time from the genuine preset one.
>
> * * *
>
> Reference is now made to FIG. 4 which is a block diagram that illustrates an authenticator 100, constructed and operative in accordance with a preferred embodiment of the present invention. The authenticator 100 comprises a *secure time generator 104*, a storage device 106 and a function executor 102 which has means for inputting the following information elements: the transmitted information, the destination address, *a time indication generated by the secure time generator 104*, and a dispatch completion indication. Optionally, additional information elements can be provided as well.
>
> * * *
>
> A related embodiment can utilize a Time Stamping Service (TSS) such as the *Digital Notary System (DNS)* provided by Surety Technologies Inc. [1.10],[8] which

[7] Though not of consequence in this Memorandum Opinion and Order, "UTC" presumably refers to "Coordinated Universal Time," which is also known as "Zulu" time.

[8] Citing "'Applied Cryptography (2nd Edition)', (Schneier[,] Bruce, John Wiley & Sons, 1996)," "Chapter 4 Section 4.1, pp. 75-79."

> has been proposed by Haber et al. in their U.S. patent documents [2].[9] The certificate 740 or any portion thereof (such as the signature 742) can be sent to the DNS to be time stamped. Alternatively, an embodiment of the present invention could internally implement the DNS scheme. The DNS generates a certificate authenticating the certificate 740. Utilizing such time stamping schemes is of great advantage, since the DNS generated certificates are virtually unforgeable, and there is no need to deposit copies of the certificates with trustees. Since in this case the DNS time stamps the certificate 740 anyway, the service 750 itself optionally need not add the time indication 720.

('219 Patent at 7:12-28, 13:8-18 & 16:60-17:7 (emphasis added) (square brackets in original).)

As to amended Claim 71, Defendants argue that this disclosure fails to disclose structure for performing the recited function of providing an indicia of a time of "successful" transmission. On one hand, validity issues, such as lack of written description and lack of enablement, are generally not considered as part of claim construction. *Phillips*, 415 F.3d at 1327 ("[W]e have certainly not endorsed a regime in which validity analysis is a regular component of claim construction."). On the other hand, a "structure disclosed in the specification is 'corresponding' structure only if the specification or prosecution history clearly links or associates that structure to the function recited in the claim." *Medtronic, Inc. v. Advanced Cardiovascular Sys., Inc.*, 248 F.3d 1303, 1311 (Fed. Cir. 2001); *Telcordia*, 612 F.3d at 1376.

On balance, although the reexamination amended Claim 71 to recite "successful" transmission, the structure disclosed in the specification performs the recited function by providing a time indication. As to Defendants' proposal that the time indication need not be provided by electronic means, the claim recites "transmission "via an electronic communication network" and "the dispatch being electronically transmitted." The time indication is therefore electronic. As quoted above, the specification discloses multiple corresponding structures:

[9] Citing "U.S. Pat. Nos. 5,136,646, 5,136,647, and 5,373,561."

internal clock 50; a communication network server; secure time generator 104; and the Digital Notary System (DNS). These structures should be included in the Court's constructions as alternatives. *See Ishida Co., Ltd. v. Taylor*, 221 F.3d 1310, 1316 (Fed. Cir. 2000) (noting that a patent can "disclose[] alternative structures for accomplishing the claimed function"). As to the definiteness requirement, no further detail is required. Defendants have thus failed to demonstrate a lack of corresponding structure in the specification.

The Court therefore hereby construes the disputed terms as set forth in the following chart:

"means for providing an indicia relating to a time of transmission of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient" ('219 Patent, Claim 71 (original))	**Function:** **"providing an indicia relating to a time of transmission of the dispatch, said time related indicia being provided in a manner resistant to or indicative of tampering by either of the sender and the recipient"** **Corresponding Structure:** **"(1) internal clock 50, and equivalents thereof; (2) a communication network server, and equivalents thereof; (3) secure time generator 104, and equivalents thereof; or (4) the Digital Notary System (DNS), and equivalents thereof"**
"means for providing an indicia of a time of successful transmission of the dispatch to the receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient" ('219 Patent, Claim 71 (amended))	**Function:** **"providing an indicia of a time of successful transmission of the dispatch to the receiving system, said time related indicia being recorded by the authenticator and provided in a manner resistant to or indicative of tampering by either of the sender and the recipient"** **Corresponding Structure:** **"(1) internal clock 50, and equivalents thereof; (2) a communication network server, and equivalents thereof; (3) secure time generator 104, and equivalents thereof; or (4) the Digital Notary System (DNS), and equivalents thereof"**

I. "means for securing at least part of the authentication data against tampering of the sender and the recipient" ('219 Patent, Claim 71)

Plaintiffs' Proposal	**Defendants' Proposal**
The function of this limitation is securing at least part of the authentication data so that it is resistant to or indicative of tampering. The corresponding structure is a storage unit 54 or storage device 106 that may be a write-once read-many (WORM) device such as an optical disk or a Programmable Read-Only Memory device, it may be enclosed within a securable device, or it may be provided with read-only access privilege. Alternatively, the storage unit or storage device may store authentication information using a compression, private or public key encryption or scrambling technique, a password, or a combination thereof.	Amazon, PayPal, Zix, DocuSign, ReadNotify, Chris Drake, RightSignature, and Farmers propose: This language triggers Sec. 112, ¶ 6. Function: securing at least part of the authentication data against tampering by either the sender or the recipient, with the authenticator functioning as a non-interested third party Structure: Fig. 1 (see secure file 36); 219.5:44-50; Figs. 2 & 3 (see item 54); 219.9:55-67 (encryption, compression, symmetric digital signatures, asymmetric digital signatures); 219.14:25-15:42 (fingerprint); 219.15:66-16:32 (RSA, DSA, MD4, MD5) Adobe proposes: Function: securing at least part of the authentication data against tampering of the sender and the recipient, the authenticator functioning as a non-interested third party with respect to the sender and the recipient Structure: a storage unit within the authenticator as described by 7:44-58

(Dkt. No. 211, Ex. I, at 18-19; Dkt. No. 259, 1/31/2013 P.R 4-5(d) Joint Claim Construction Chart, at 36.)

(1) The Parties' Positions

Plaintiffs argue that the corresponding structure is explicitly disclosed in the specification of the '219 Patent at column 7, lines 41-58. (Dkt. No. 251, at 16.)

Defendants respond that "[t]he parties agree that the corresponding structure includes digital electronic storage devices that secure the data against tampering," but "the specification also discloses using a locked file cabinet to secure the authentication data against tampering." (Dkt. No. 253, at 19-20.)

Plaintiffs reply that whereas "[t]he function of this claim language recites 'data[,]' [t]he patent's file cabinet disclosure only takes paper-stuffed envelopes, not 'data.'" (Dkt. No. 257, at 6.)

(2) Analysis

Plaintiffs have identified the following passage as disclosing corresponding structure:

> The storage unit 54 is used for storing the information 60 and/or the dispatch information, including the address 62, the time indication 66, and optionally the transmission completion indication 64. Typically, the storage unit 54 is relatively secure, such that the authentication-information contained therein is assumed unchangeable. For example it may be a Write-Once-Read-Many (WORM) device such as an optical disk or a Programmable Read-Only Memory (PROM) device, it may be enclosed within a securable device, or it may be provided with read-only access privilege. Alternatively, the authentication-information is stored in a secure manner, for example using a compression, private or public key encryption or scrambling technique, a password, or a combination thereof, such as those employed by the widely used RSA encryption method, and by the PKZIP(tm) program from PKWARE Inc., Glendale Wis., U.S.A., and where the "securing" procedure, key or password are unknown to any interested party.

('219 Patent at 7:41-58.)

Defendants have identified, in addition, the following structures:

> Preferably, the clerk 20 secures the copies 24 and 34 in a manner that makes it difficult to modify or replace the information contained therein, for example by marking the pages of the copy 24 with the dispatching service's signature, stamp or seal, by spreading each page with invisible or other ink, by sealing the envelope 32 or by retaining them in the service's secure file 36 and so forth.

(*Id.* at 5:44-50.)

> Similarly, information transmitted in a computer network or electronic mail system can be authenticated, for example, by having a file server or mail manager (whose time generator is considered secure) store the transmitted information together with its associated dispatch information in a secure manner. One embodiment of secure storage is that which has read-only privileges. Alternatively, such read-only effect can also be obtained by having the authentication-information encrypted with the authenticator's private key: everybody can decrypt it using the authenticator's public key, but no interested party can change it without such action being detectable.

(*Id.* at 9:56-67.)

> Also, part of the securing methods which were described for FIG. 2 include for example encryption and compression methods which formally relate to mathematical association functions such as ENCRYPT(a1, . . . , aj) and COMPRESS(a1, . . . , aj). Occasionally, there is a need for reconstructing some or all of the secured mathematically associated information elements, for example for providing them to an output unit or to the comparator of the verification mechanism. Since some compression and encryption functions (as some other functions) are reversible, they are typically used when reconstruction of the elements is needed. (A function G is considered reversible if there exists a function H such that H(G(x))=x, and the function H is called the inverse function of G).
>
> As discussed hereinabove, a mathematical association function can generally comprise a single function, or the composition of two or more functions. For example, the function ENCRYPT(a1, . . . , aj) comprises a single function ENCRYPT, which is reversible, and its inverse function is DECRYPT. Another function COMPRESS (ENCRYPT(a1),C.R.C(a2, . . . , aj)) is the composition of three functions--COMPRESS, ENCRYPT and C.R.C, where the first two are reversible and their inverse function are DECOMPRESS (which yields the set comprising ENCRYPT(a1) and C.R.C(a2, . . . , aj)), and DECRYPT (which yields the element a1) respectively. The C.R.C function however, is not reversible.
>
> Formally, if a function Fi comprises one or more functions, some of which are reversible, a set C comprising one or more information elements c1, . . . , ck can be generated, where this set C is expressive as a function I applied to the result information element bi of the function Fi, where this function I comprises the inverse function of one or more of these reversible functions.
>
> While the authentication methods described hereinabove refer mostly to symmetric digital signatures, a preferred authentication method may be obtained using public-key digital signatures. A major advantage of public-key digital signatures over symmetric digital signatures is that they enable any third party (such as a judge), to verify the authenticity of both the data and the signer (where by using symmetric digital signatures, only a designated authenticator such as a secure device or a trusted third party, which have knowledge of the function, secret keys/codes etc., can perform the verification). The data is guaranteed not to be tampered with, and furthermore, once the data is signed, the signer is actually "committed" to it and cannot later repudiate his commitment to the digitally signed data, for only the signer which has sole knowledge of his private key could have created the signature, thus allowing such data to be legally binding.
>
> Typically, public-key digital signatures generation and data authentication i[s] performed in the following manner: a computation involving the signer's private key and the data, which can comprise various elements such as the dispatched

message, the time indication, the destination address, and so forth is performed; the output is the digital signature, and may be attached to the data or separated therefrom. In later attempt of verification of the data, some computation involving the purported data, the signature, and signer's public key is performed. If the results properly hold in simple mathematical relation, the data is verified as genuine; otherwise, it may be forged or may have been altered or otherwise tampered with.

Since the signing process using the whole (plain) data is generally time consuming and the signature consumes a considerable amount of storage space, typically a relatively unique representation (also called a "fingerprint" or the "message digest") of the data is first generated using a process in which the data is "condensed" or "hashed", for example by means of a one-way hash function into a relative small value, thereby fixing its contents, and the signing process is performed on the fingerprint, resulting in an equivalent effective authentication. Therefore, the term digital signature herein refers to the digital signature of either the plain data element(s) or of any representation (function) thereof.

As described hereinabove, the fingerprint of a series of data elements can be generated thereby fixing their contents and associating them with each other. Since public-key digital signatures belong to the "Hiding Class", and since they further own the property that they can be generated with one key (such as the private key), and provide for later non-repudiable verification using another matching key (such as the public key), the usage of such functions for the purposes of the present invention is therefore of great advantage.

(*Id.* at 14:25-15:42.)

Digital signatures can be generated in system 700 for example by means of a verifiable public-key algorithm such as RSA or DSA. Fingerprints can be generated for example by means of a one-way hash function such as MD4 or MD5.

The service 750 forwards the message 701 to the recipient 799 using the address 704. The service 750, preferably after assuring that the message has been successfully delivered, adds (e.g., appends) a dispatch time indication 720 to the message 702 and the address 704, as well as information 708 indicating the success (or failure) of the message delivery. Obviously, additional dispatch information elements, such as a sequential dispatch number, the sender, recipient and the service identification information and so forth may be added as well.

The service 750 then associates the above data elements for example by generating their fingerprint, which is then signed using the service's private key 752, to produce the service's signature 742. [S]igning the fingerprint can reduce the resulting signature 742 computation time, transmission bandwidth and storage space. The service then provides back to the sender 701 a service's generated

> certificate 740 comprising the service's signature 742 and optionally various dispatch information elements from which it has been generated (there is no need to provide the message 702 and address 704 since they are already with the sender 701), thus the certificate 740 is typically tiny.
>
> Thus, for example, using RSA to generate the signature, if M is the dispatched message 702, A is the address 704, T is the time indication 720, I is the delivery information 708, and Ka is the authentication service's RSA private key, then the following is a sample calculation of S--the signature 742:
>
> $$RSA(S, PBKa) = MD5(U(T', I', M', A'))$$

(*Id.* at 15:66-16:32.)

On balance, the proposals by Plaintiffs and Defendants include more detail than is necessary for performing the claimed function. *See Acromed Corp. v. Sofamor Danek Group Inc.*, 253 F.3d 1371, 1382 (Fed. Cir. 2001) (regarding a screw as corresponding structure, finding that "[t]o limit the body portion to a diameter at least as large as the crest diameter of the second externally threaded portion would be to impermissibly import into the claim limitation specific dimensions of a preferred embodiment that are unnecessary to perform the claimed function . . ."). The Court therefore rejects both sides' proposals.

As to the proper construction, the primary dispute between the parties is whether the corresponding structure includes, as an alternative, the "secure file 36." *See Ishida*, 221 F.3d at 1316 (noting that a patent can "disclose[] alternative structures for accomplishing the claimed function"). The body of Claim 71 of the '219 Patent recites "the communication network," which has its antecedent basis in the recitation of "electronic communication network" in the preamble. The parties have agreed that "terms that appear in both the preamble and the body of a claim serve as claim limitations" (Dkt. No. 211, 11/29/2012 Joint Claim Construction and Prehearing Statement, at 5), so the recited communication network must be electronic. The body

of the claim also recites "the dispatch being electronically transmitted to said receiving system." In light of these electronic limitations in the claim, a person of ordinary skill in the art would conclude that the "secure file 36," which refers to a physical file cabinet, is not corresponding structure for the "means for securing" in Claim 71. Defendants' proposal in that regard is hereby expressly rejected.

The Court therefore hereby finds that for the term **"means for securing at least part of the authentication data against tampering of the sender and the recipient,"** the function is **"securing at least part of the authentication data against tampering by either the sender or the recipient"** and the corresponding structure is **"storage unit 54 or storage device 106, and equivalents thereof."**

J. Remaining Terms of the Feldbau Patents

Plaintiffs submit that:

> RPost believes that the vast majority of the remaining disputes will be predetermined upon the Court's resolution of the six central disputes that RPost has identified above. RPost therefore suggests three possible approaches for handling the remainder of the disputed terms. One, the Court may resolve the central disputes noted here and direct the parties to prepare an agreed order expressing how those resolutions have determined the remainder. Two, after considering the central disputes noted here, Defendants' response, RPost's reply, and arguments at the Markman Hearing, the Court may proceed workmanlike through the Local Rule 4-5(d) Claim Construction Chart and issue a comprehensive decision announcing the respective rulings of the Court. Or three, if Defendants agree and if the Court permits, the remainder of the disputes may be postponed until the jury instruction conference.

(Dkt. No. 251, at 17.)

Defendants respond that "any additional claim construction disputes may be addressed either in the context of a motion for summary judgment and/or in the jury instructions." (Dkt. No. 253, at 30.)

The parties January 31, 2013 P.R. 4-5(d) Joint Claim Construction Chart includes a "Table One," which "focuses on the primary terms in dispute for the Feldbau patents" as used in Claim 35 of the '334 Patent and Claim 30 of the '219 Patent, followed by a "Table Two" that "includes all other asserted claims, and reflects the additional terms in dispute." (Dkt. No. 259, at 4; *see id.*, at 8-18 ("Table One") & 19-39 ("Table Two").)

The parties' approach is unconventional. Typically, parties present some grouping of terms in their briefing or otherwise explain how their proposals for certain terms rise or fall based on the Court's construction of other terms. Instead, the parties here present competing proposals for several terms that are not briefed by either side. Further adding to the confusion, some of the terms briefed by the parties are not included in the parties' "Table One" that sets forth the "primary terms in dispute." (*See, e.g.*, Dkt. No. 151, at 15-17; Dkt. No. 259, at 32-36 (means-plus-function terms that have been briefed are included in "Table Two" of "additional," non-"primary" terms in dispute).)

The parties filed a Joint Motion for Page Limits for Claim Construction Briefing (Dkt. No. 227) requesting leave for the parties to file claim construction briefs exceeding the Court's standard page limits. The Court denied that motion. (Dkt. No. 229, 12/21/2012 Order.) When Plaintiffs disregarded the Court's Order by filing claim construction briefing in excess of the Court's standard page limits, the Court struck Plaintiffs' briefing. (Dkt. No. 249, 1/8/2013 Order (striking Dkt. Nos. 242 & 244).) The page limitations do not warrant excusing the parties from presenting claim term disputes in a manner that can be properly evaluated and ruled upon.

The relevant inquiry, from the Court's perspective, is whether a dispute has been properly presented to the Court. The Court declines to speculate regarding the arguments that would have been presented if the parties had briefed a particular purportedly disputed term. Instead, the

Court rules upon the claim construction disputes that have been briefed and does not address any so-called "additional terms" that have not been briefed by either side.

K. Remaining Issues for the Feldbau Patents

Defendants propose that the Court enter several findings as to the "Claims as a Whole." (*See* Dkt. No. 259, 1/31/2013 P.R. 4-5(d) Claim Construction Chart, at 37-39.) Defendants have presented no authority for a process by which the Court rules on disputes in the abstract, so to speak, divorced from any disputed term. The Court declines to adopt any such practice here. The parties' proposals as to the "Claims as a Whole" are therefore hereby expressly rejected.

V. CONSTRUCTION OF DISPUTED TERMS IN THE '624 "TOMKOW" PATENT

The Abstract of the '624 Patent states:

> A server transmits a message from a sender to a recipient. The server receives from the recipient an attachment relating to the message route between the server and the recipient. The server transmits to the sender the message and the attachment and their encrypted digital fingerprints and expunges the transmitted information. To subsequently authenticate the message and the attachment, the sender transmits to the server what the server has previously transmitted to the sender. The server then prepares a digital fingerprint of the message and decrypts the encrypted digital fingerprint of the message and compares these digital fingerprints to authenticate the message. The server performs the same routine with the attachment and the encrypted digital fingerprint of the attachment to authenticate the attachment[. T]he recipient replies to the sender's message through the server. The server records proof of the delivery and content of the reply to the sender and the recipient.

A. "a message" (Claim 1)

Plaintiffs' Proposal	**Defendants' Proposal**
"an electronic message"	"an email from the sender to the recipient"

(Dkt. No. 211, Ex. J, at 1.)

(1) The Parties' Positions

Plaintiffs argue that "a message" is electronic but should not be limited to email. (Dkt. No. 261, at 17.) Plaintiffs note that whereas the preamble of Claim 1 of the '624 Patent refers to

email, the body of the claim recites "a message." (*Id.*, at 18.) Plaintiffs urge that although the preferred embodiments relate to email, the claims should not be limited by preferred embodiments. (*Id.*) Plaintiffs also argue that Defendants' proposal improperly requires a message "from the sender to the recipient" whereas "[t]he plain language of the claims, however, recites that the message passes from the sender to a server or from the server to a recipient." (*Id.*)

Defendants respond that "[t]he 'message' that is recited in the claim body, and that is the subject of the 'manually initiated reply' recited in the preamble, is . . . the same as the 'email' recited in the preamble." (Dkt. No. 253, at 30.)

Plaintiffs reply that "[t]he body [of] claim 1 separately recites 'a message' and does not rely on the preamble for antecedent basis or structural elements." (Dkt. No. 257, at 10.) Plaintiffs conclude that "Defendants' attempt to limit the message recited in the claim to the email referred to in the preamble must fail." (*Id.*)

(2) Analysis

Claim 1 of the '624 Patent recites (emphasis added):

> 1. A method of providing a recipient of an email with proof of the transmission, receipt and content of a reply to the email that is manually initiated by the recipient, comprising:
>
> receiving a *message* from a sender at a server displaced from the recipient;
>
> assigning a unique identification of the *message* by the server;
>
> storing the unique identification of the *message* in a database;
>
> adding a "mailto" link to the *message* and also adding an invitation to click on the link if the recipient wishes to receive proof of transmission or delivery of the reply;
>
> transmitting the *message* from the server to the recipient;
>
> generating a manually initiated reply to the *message* at the recipient, the manually initiated reply including a request from the recipient to receive proof of transmission or delivery of the manually initiated reply to the sender by clicking on the "mailto" link included in the *message*;
>
> transmitting the manually initiated reply to the sender through the server;
>
> receiving the manually initiated reply at the server;

> processing the request by the recipient to receive proof of transmission or delivery of the manually initiated reply to the sender;
>
> transmitting the manually initiated reply by the recipient to the sender in a manner wherein the server receives an indication that the reply is transmitted or delivered to the sender; and,
>
> transmitting the indication that the reply is transmitted or delivered to the sender to the recipient.

The Background of a Preferred Embodiment of the Invention discloses:

> In co-pending application Ser. No. 09/626,577, filed by Dr. Terrance A. Tomkow and assigned of record to the assignee of record of this application, a system and method are disclosed and claimed for reliably verifying via secure and tamper-proof documentation the content and delivery of *an electronic message such as an e-mail*. Ideally, the invention disclosed and claimed in co-pending application Ser. No. 09/626,577 will give *e-mail and other electronic messages* a legal status on a par with, if not superior to, that of registered United States mail.

('624 Patent at 2:67-3:5 (emphasis added).) A person of ordinary skill in the art would therefore readily understand that the term "message" can include email but is not limited to email.

> The word "email" appears only in the preamble of Claim 1 of the '624 Patent.
>
> In general, a preamble limits the invention if it recites essential structure or steps, or if it is "necessary to give life, meaning, and vitality" to the claim. *Pitney Bowes*[*, Inc. v. Hewlett-Packard Co.*], 182 F.3d [1298,] 1305 [(Fed. Cir. 1999)]. Conversely, a preamble is not limiting "where a patentee defines a structurally complete invention in the claim body and uses the preamble only to state a purpose or intended use for the invention." *Rowe v. Dror*, 112 F.3d 473, 478, 42 USPQ2d 1550, 1553 (Fed. Cir. 1997).

Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc., 289 F.3d 801, 808 (Fed. Cir. 2002). Although certain terms in the body of Claim 1, such as "the recipient" and "the reply," derive antecedent basis from "a recipient" and "a reply" in the preamble, as quoted above, the word "email" does not appear outside of the preamble and is not necessary to "give life, meaning, and vitality" to the claim. *Id.*

The Court therefore adopts Plaintiffs' proposal and hereby construes **"a message"** to mean **"an electronic message."**

B. "a 'mailto' link" (Claim 1)

Plaintiffs' Proposal	Defendants' Proposal
"a link that generates an electronic message addressed to an embedded email address"	"an HTML[10] link that includes a URL[11] that specifies the 'mailto' protocol, e.g., …"

(Dkt. No. 211, Ex. J, at 1.)

(1) The Parties' Positions

Plaintiffs argue that Defendants' proposal should be rejected because "[i]t is evident from the plain language that claim 1 is not intended to be limited to any particular language or protocol." (Dkt. No. 251, at 19.) Plaintiffs also argue claim differentiation as to independent Claim 7, which recites "adding an HTML link in the message." (*Id.*)

Defendants respond that "mailto" is a "term of art," as the patentee indicated by placing "mailto" in quotation marks in Claim 1. (Dkt. No. 253, at 27.) Defendants argue that the specification expressly defines "a 'mailto' link" as being an "HTML" link. (*Id.*, at 28.) Defendants also argue that Figure 12, cited by Plaintiffs, shows a message in "MIME"[12] format but in which the message body is in HTML format. (*Id.*) Defendants submit that "the 'mailto' link must have some format, which the specification teaches is HTML." (*Id.*, at 29.) Defendants further urge that "the specification describes the 'mailto' link as using the 'mailto' protocol," which is "defined by the standards document RFC 2368, titled 'The mailto URL scheme.'" (*Id.* (citing Ex. S).) Defendants conclude that no other protocol is described or enabled in the

[10] "HTML" presumably refers to HyperText Markup Language, which is commonly used for creating web pages.

[11] "URL" presumably refers to Uniform Resource Locator, which is also sometimes referred to as a web address and which is a reference to a resource on a computer network.

[12] "MIME" presumably refers to Multipurpose Internet Mail Extensions, which is a standard for the format of email.

specification and that "an enabled construction must be adopted over a non-enabled construction." (*Id.* (citing *Athletic Alternatives, Inc. v. Prince Mfg., Inc.*, 73 F.3d 1573, 1581 (Fed. Cir. 1996)).)

Plaintiffs reply that "[i]f the inventor intended to claim such a [HTML 'mailto'] link, then he would have specified HTML as he did in claim 7 and in the specification." (Dkt. No. 257, at 10.)

At the February 14, 2013 hearing, when the Court inquired of Plaintiffs why the term "mailto" appears within quotation marks in Claim 1 if not to denote some special meaning, Plaintiffs responded that the purpose is unknown but might have been to signal similarity, not identity to the mailto protocol. Plaintiffs re-urged their argument that the patentee deliberately chose *not* to recite an "HTML 'mailto' link" in Claim 1 and instead recited a generic "'mailto' link" in Claim 1 and an "HTML link" in Claim 7.

(2) Analysis

Claim 1 of the '624 Patent recites, in relevant part (emphasis added):

> 1. A method of providing a recipient of an email with proof of the transmission, receipt and content of a reply to the email that is manually initiated by the recipient, comprising:
>
> receiving a message from a sender at a server displaced from the recipient;
>
> assigning a unique identification of the message by the server;
>
> storing the unique identification of the message in a database;
>
> *adding a "mailto" link to the message* and also adding an invitation to click on the link if the recipient wishes to receive proof of transmission or delivery of the reply;
>
> transmitting the message from the server to the recipient;
>
> generating a manually initiated reply to the message at the recipient, the manually initiated reply including a request from the recipient to receive proof of transmission or delivery of the manually initiated reply to the sender by *clicking on the "mailto" link included in the message*; . . . .

The specification discloses:

> This description is not to be taken in a limiting sense, but is made merely for the purpose of illustrating the general principles of the invention. The section titles and overall organization of the present detailed description are for the purpose of convenience only and are not intended to limit the present invention. Accordingly, the invention will be described with respect to e-mail messaging systems that use the internet network architecture and infrastructure. It is to be understood that *the particular message type and network architecture described herein is for illustration only*; the invention also applies to other electronic message protocols and message types using other computer network architectures, including wired and wireless networks.

('624 Patent at 8:39-44 (emphasis added).)

> 1504. For each copy of the message delivered to each destination, the system includes *an HTML "MAILTO" link* in the message together with an invitation to click on the link if the recipient wishes to receive proof of transmission or delivery of the reply. The address included in the *MAILTO link* is a fictitious address at a domain controlled by the sender or the sender's agent. The address is formed from the message and destination IDs. Thus if the message ID was "ABC123" then, for a copy of the message to be delivered to a destination "2" of the message, the link might appear as "Message Message! Destination! at rpost.net".
>
> To send a registered reply, click
> here
>
> which would direct the reply to the server for the "rpost.net" domain (hereinafter "the RPost Server").
>
> 1505. The message is then transmitted.
>
> 1506. When a recipient of the message, *using an HTML enabled mail browser, clicks on the link*, the browser will open the recipient's default mail client with a message already addressed to the embedded address. The recipient composes a reply and sends it to the fictitious address.

(*Id.* at 30:66-31:18 (emphasis added).)

Despite the above-quoted general statement that "the particular message type and network architecture described herein is for illustration only," the disclosure of "an HTML 'MAILTO' link" (*id.*), with "mailto" in quotation marks, is persuasive evidence that a person of

ordinary skill in the art would understand the term "'mailto' link" in Claim 1 to refer to an HTML "mailto" link. (*Id.*)

Plaintiffs rely on claim differentiation as to independent Claim 7, which recites "an HTML link." Notably, Claim 7 does not recite an "HTML 'mailto' link," and Claim 7 also recites many additional limitations (emphasis added):

> 7. A method of transmitting a message from a sender to a recipient through a server displaced from the recipient, including the steps at the server of:
>
> receiving the message at the server from the sender,
>
> providing the message with a unique identification by the server,
>
> providing the sender with a unique identification related to the unique identification of the message by the server,
>
> transmitting the message from the server to the recipient,
>
> adding an *HTML link* in the message and also adding instructions to click on the link if the recipient wishes to receive proof of transmission or delivery of the reply,
>
> storing the unique identification of the message and the sender including an address of the sender in a database by the server,
>
> initiating manually a reply to the message by the recipient clicking on the link in the message, the reply including a request from the recipient to receive proof of delivery of the reply to the sender and proof of content of the reply, the reply also including the unique identification,
>
> receiving the reply at the server,
>
> locating in the database by the server the identification of the message and the sender using the unique identification in the reply, and
>
> transmitting to the sender through the server any the [*sic*] reply by the recipient to the sender in a manner wherein the server receives an indication that the reply is delivered to the sender and proof of the content of the reply,
>
> transmitting to the recipient the indication that the reply is delivered to the sender and proof of the content of the reply.

On balance, Plaintiffs' claim differentiation argument is unpersuasive. *See, e.g.*, *Rembrandt Techs., LP v. Cablevision Sys. Corp.*, No. 2012-1022, 2012 WL 4017470, at *9 (Fed. Cir. Sept. 13, 2012) ("There is no reason to apply the doctrine of claim differentiation, however, where, as here, the district court's construction does not render any claim redundant or superfluous."); *Kemco Sales, Inc. v. Control Papers Co., Inc.*, 208 F.3d 1352, 1363 (Fed. Cir. 2000); *Wenger Mfg., Inc. v. Coating Mach. Sys., Inc.*, 239 F.3d 1225, 1233 (Fed. Cir. 2001) ("Claim

differentiation, while often argued to be controlling when it does not apply, is clearly applicable when there is a dispute over whether a limitation found in a dependent claim should be read into an independent claim, and that limitation is the only meaningful difference between the two claims.").

As to the examples set forth in an extrinsic Internet standards document that describes the mailto protocol, the absence of HTML tags in the examples (such as "<mailto:chris@example.com>") is not of consequence here because the examples are described as being mailto "URLs," not mailto links. (Dkt. No. 253, Ex. S, RFC 2368, "The mailto URL scheme," at 4-5.)

Finally, Defendants' proposal of "e.g., …" is unnecessary and might be perceived as limiting. Defendants' proposed example should therefore be omitted from the Court's construction.

The Court therefore hereby construes **"a 'mailto' link"** to mean **"an HTML link that includes a URL that specifies the 'mailto' protocol."**

C. "an invitation to click on the link" (Claim 1)

Plaintiffs' Proposal	**Defendants' Proposal**
"a suggestion presented to the user to click on the link"	"text embedded in the email that invites the recipient to click the 'mailto' link"

(Dkt. No. 211, Ex. J, at 1.)

(1) The Parties' Positions

Plaintiffs argue that "[n]either the claim language nor the specification place any limits on the type of invitation." (Dkt. No. 251, at 19.)

Defendants respond that because "[t]he 'mailto' link and the invitation are 'added . . . to the message," "[i]t is thus clear that the invitation must be part of (or embedded) in the message,

as required by Defendants' construction." (Dkt. No. 253, at 30.) Defendants submit that "Plaintiffs' construction, on the other hand, would seem to allow any suggestion (even a free-floating one) that is presented to the user, even though such a suggestion would never have been 'added' to the message, as required by the plain language of the claims." (*Id.*)

Plaintiffs reply that "Claim 1 says that the invitation is added but it does not say that it is added to the message. Thus, the invitation does not need to be part of the message body, it can, for example, be part of the link." (Dkt. No. 257, at 10.)

(2) Analysis

Claim 1 of the '624 Patent recites, in relevant part (emphasis added):

> 1. A method of providing a recipient of an email with proof of the transmission, receipt and content of a reply to the email that is manually initiated by the recipient, comprising:
>
> receiving a message from a sender at a server displaced from the recipient;
>
> assigning a unique identification of the message by the server;
>
> storing the unique identification of the message in a database;
>
> *adding a "mailto" link to the message and also adding an invitation to click on the link if the recipient wishes to receive proof of transmission or delivery of the reply*;
>
> transmitting the message from the server to the recipient;
>
> generating a manually initiated reply to the message at the recipient, the manually initiated reply including a request from the recipient to receive proof of transmission or delivery of the manually initiated reply to the sender by *clicking on the "mailto" link included in the message*; . . . .

The specification discloses:

> Although such is not necessary to the practice of the invention, the message may be tagged to denote the fact that the message has been made of record, such as by inserting the words "Made of Record" or at the beginning of the "subject" line of the message, by appending a tag such as,
>
> > "This message has been made of record with RPost. Visit our web site at www.RPost.com for additional information."
>
> at the end of the original message or other tagging. Additionally, the tag may contain instructions, World Wide Web addresses, or *links that invite and allow the*

recipient to send a reply made of record to the message by linking to a Web Page from which messages made of record may be composed and sent.

(*Id.* at 10:36-49 (emphasis added).)

> 1504. For each copy of the message delivered to each destination, the system *includes an HTML "MAILTO" link in the message together with an invitation to click on the link if the recipient wishes to receive proof of transmission or delivery of the reply*. The address included in the MAILTO link is a fictitious address at a domain controlled by the sender or the sender's agent. The address is formed from the message and destination IDs. Thus if the message ID was "ABC123" then, for a copy of the message to be delivered to a destination "2" of the message, the link might appear as "Message Message! Destination! at rpost.net".
>
> To send a registered reply, click
> here
>
> which would direct the reply to the server for the "rpost.net" domain (hereinafter "the RPost Server").
>
> 1505. The message is then transmitted.
>
> 1506. When a recipient of the message, using an HTML enabled mail browser, clicks on the link, the browser will open the recipient's default mail client with a message already addressed to the embedded address. The recipient composes a reply and sends it to the fictitious address.

(*Id.* at 30:66-31:18 (emphasis added).) Thus, as recited in Claim 1 of the '624 Patent and as supported by the above-quoted passages from the specification, the invitation is "in the message." Defendants have failed to demonstrate, however, that the invitation must be "text" rather than, for example, an icon or a graphic.

The Court therefore hereby construes **"an invitation to click on the link"** to mean **"a suggestion embedded in the message that invites the recipient to click the 'mailto' link."**

D. "a manually initiated reply" (Claim 1)

Plaintiffs' Proposal	Defendants' Proposal
"a reply initiated by a user action"	"a reply generated by the manual action of the recipient clicking on the 'mailto' link"

(Dkt. No. 211, Ex. J, at 1.)

(1) The Parties' Positions

Plaintiffs argue that Defendants' proposed construction "improperly limits the invention to actions performed by hand, specifically using the hands to click on the 'mailto' link." (Dkt. No. 251, at 20.) Plaintiffs argue that perhaps "voice commands" or some other hands-free mechanism could be used because "the inventor used the term 'manually' to distinguish systems that automatically generate delivery status notifications, not systems that are operated by hand." (*Id.*)

Defendants respond that "the claim language requires that the manually initiated reply be generated by the recipient." (Dkt. No. 253, at 26.) Defendants cite statements in the specification and the prosecution history that a recipient must "click[] on the link." (*Id.*, at 27 (discussing '624 Patent at 31:15-20; Dkt. No. 253, Ex. Q, 10/8/2009 Preliminary Amendment, at 8).) Finally, Defendants submit that Plaintiffs' argument regarding using voice commands instead of clicking by hand is a "a red herring, which Plaintiffs are using as an excuse to read out the plain language of the claim, including 'manually' and 'by clicking on the 'mailto' link.'" (*Id.*, at 27.)

Plaintiffs reply that "Defendants' assertion that the manually initiated [reply] is generated by the recipient is at odds with the plain language of the claim," which recites a reply "at the recipient," not by the recipient. (Dkt. No. 257, at 9.) Plaintiffs also argue that the "by clicking" clause modifies "including a request from the recipient to receive proof of transmission or

delivery of the manually initiated reply to the sender," not "generating a manually initiated reply." (*Id.*, at 9-10.)

At the February 14, 2013 hearing, Plaintiffs emphasized that "manually" does not mean "by hand" but instead is contrasted with automatically, as set forth in the prosecution history: "Applicant claims a reply that is *manually* initiated by the recipient of the email, which is completely different from an *automatic* DSN [(Delivery Status Notification)] generated by a recipient[']s email system." (Dkt. No. 251, Ex. 10, 1/12/2009 Amendment, at 8 (emphasis added).) In response, Defendants explained they are proposing that a "click" must be something like a mouse click or a finger touch because any other interpretation would read "clicking" out of the claim.

(2) Analysis

Claim 1 of the '624 Patent recites (emphasis added):

> 1. A method of providing a recipient of an email with proof of the transmission, receipt and content of *a reply to the email that is manually initiated by the recipient*, comprising:
>
> receiving a message from a sender at a server displaced from the recipient;
>
> assigning a unique identification of the message by the server;
>
> storing the unique identification of the message in a database;
>
> adding a "mailto" link to the message and also adding an invitation to click on the link if the recipient wishes to receive proof of transmission or delivery of the reply;
>
> transmitting the message from the server to the recipient;
>
> *generating a manually initiated reply to the message at the recipient, the manually initiated reply including a request from the recipient to receive proof of transmission or delivery of the manually initiated reply to the sender by clicking on the "mailto" link included in the message*;
>
> transmitting *the manually initiated reply* to the sender through the server;
>
> receiving *the manually initiated reply* at the server;
>
> processing the request by the recipient to receive proof of transmission or delivery of *the manually initiated reply* to the sender;
>
> transmitting *the manually initiated reply* by the recipient to the sender in a manner wherein the server receives an indication that the reply is transmitted or delivered to the sender; and,

transmitting the indication that the reply is transmitted or delivered to the sender to the recipient.

The specification discloses:

> 1504. For each copy of the message delivered to each destination, the system includes an HTML "MAILTO" link in the message together with an invitation to *click on the link* if the recipient wishes to receive proof of transmission or delivery of the reply. The address included in the MAILTO link is a fictitious address at a domain controlled by the sender or the sender's agent. The address is formed from the message and destination IDs. Thus if the message ID was "ABC123" then, for a copy of the message to be delivered to a destination "2" of the message, the link might appear as "Message Message! Destination! at rpost.net".
>
> To send a registered reply, click
> here
>
> which would direct the reply to the server for the "rpost.net" domain (hereinafter "the RPost Server").
>
> 1505. The message is then transmitted.
>
> 1506. *When a recipient of the message, using an HTML enabled mail browser, clicks on the link, the browser will open the recipient's default mail client with a message already addressed to the embedded address.* The recipient composes a reply and sends it to the fictitious address.

(*Id.* at 30:66-31:18 (emphasis added).)

During prosecution, the patentee responded to a rejection concerning "a manually initiated reply":

> Claims 1, 9, 11 and 14 were rejected under 35 U.S.C. 112, 1st paragraph, as failing to comply with the written description requirement. More specifically, the Examiner has requested Applicant to provide the exact paragraph in the specification that supports the amendment "generating a manually initiated reply to the message at the recipient." Applicant directs the Examiner to Fig. 13, box 1506, which states "recipient clicks reply "mail to" link.["] Additional support is found in paragraphs 0330-0334. For example, paragraph 330, referring to box 1504 of Fig. 12, recites "for each copy of the message delivered to each destination, the system includes an HTML "MAIL TO" link in the message together with an invitation to click on the link if the recipient wishes to receive proof of transmission or delivery of the reply". *This section clearly indicates that a recipient must "click", a manual operation, on the link.*

> Paragraph 0334 goes even further, stating "when a recipient of the message, using a HTML enabled mail browser, clicks on the link, the browser will open the recipient's default mail client with a message already addressed to the embedded address. The recipient composes a reply and sends it to the fictitious address." Applicant respectfully submits that the subject of Fig. 13 and of paragraphs 0330-0334 full[y] support "generating a manually initiated reply to the message at the recipient."

(Dkt. No. 253, Ex. Q, 10/8/2009 Preliminary Amendment, at 8 (emphasis added).) This above-quoted prosecution history explains that a "click" is a manual action, but the patentee did not definitively state that the term "a manually initiated reply," by itself, requires initiation by a mouse click or a finger touch, as Defendants have argued. *Omega Eng.*, 334 F.3d at 1324 ("As a basic principle of claim interpretation, prosecution disclaimer promotes the public notice function of the intrinsic evidence and protects the public's reliance on *definitive* statements made during prosecution.") (emphasis added).

On balance, "clicking" is not a limitation of "a manually initiated reply." Instead, this issue is more appropriately addressed as to the larger term "generating a manually initiated reply to the message at the recipient," below.

The Court therefore adopts Plaintiffs' proposed construction and hereby construes **"a manually initiated reply"** to mean **"a reply initiated by a user action."**

E. "generating a manually initiated reply to the message at the recipient" (Claim 1)

Plaintiffs' Proposal	**Defendants' Proposal**
No need to construe; best to enter the jury instructions without explanation, with instruction that terms not specifically construed should be applied based on ordinary meaning to persons of skill in the art in the context of the intrinsic record. RPost also objects [to] any Defense construction that purports to construe this phrase but rather merely imposes limits on the phrase's scope not found in the plain language of the claims. Specifically, the plain language of this limitation does not require that this step be performed by the recipient or a manual action. Alternatively: "generating a manually initiated reply to the message at the recipient"	"clicking, by the recipient, the 'mailto' link and manually entering a message into a mail client"

(Dkt. No. 211, Ex. J, at 2.)

(1) The Parties' Positions

Plaintiffs argue claim differentiation as to Claim 11, which Plaintiffs submit "specifically claims an embodiment of the invention where the recipient composes a reply to the message in a mail client." (Dkt. No. 251, at 20-21.)

Defendants' response brief consolidates its argument on this term with argument on the term "a manually initiated reply," discussed above. (*See* Dkt. No. 253 at 26-27.)

At the February 14, 2013 hearing, Plaintiffs reiterated that in Claim 1, the phrase "by clicking on the 'mailto' link included in the message" does *not* modify "generating a manually initiated reply to the message at the recipient" but instead is part of a separate limitation. (*See* Dkt. No. 257, at 9-10.) Defendants responded that Plaintiffs proposal would read "clicking" out of the claim.

(2) Analysis

As a threshold matter, Plaintiffs' claim differentiation argument is rejected because Claim 11 is an independent claim with many distinct limitations. *See, e.g.*, *Rembrandt*, 2012 WL 4017470, at *9 ("There is no reason to apply the doctrine of claim differentiation, however, where, as here, the district court's construction does not render any claim redundant or superfluous."); *Kemco Sales*, 208 F.3d at 1363; *Wenger Mfg.*, 239 F.3d at 1233 ("Claim differentiation, while often argued to be controlling when it does not apply, is clearly applicable when there is a dispute over whether a limitation found in a dependent claim should be read into an independent claim, and that limitation is the only meaningful difference between the two claims.").

Claim 1 of the '624 Patent is reproduced above regarding the term "a manually initiated reply."

The preferred embodiment includes manually entering a message into a mail client, as Defendants have proposed:

> 1506. When a recipient of the message, using an HTML enabled mail browser, clicks on the link, the browser will open the recipient's default mail client with a message already addressed to the embedded address. The recipient composes a reply and sends it to the fictitious address.

('624 Patent at 31:15-19.) Nonetheless, Defendants have failed to justify importing that limitation into Claim 1. *Electro Med.*, 34 F.3d at 1054 ("[A]lthough the specifications may well indicate that certain embodiments are preferred, particular embodiments appearing in a specification will not be read into the claims when the claim language is broader than such embodiments.") Likewise, Defendants have failed to justify a requirement that "clicking," as recited in the claim, must refer to something like a mouse click or a finger touch.

During prosecution, however, the patentee explained that the "recipient" of the claims of the '624 Patent is "a physical person, not software":

> In paragraph 3 of the Office Action, in the section specifically directed to the Examiner's response to Applicant's previous arguments, the Examiner points to Applicant's disclosure in paragraph 0341 which states "the term recipient is also intended in the claims to include any agent of the receiver with respect to the message and attachment. Such agent may include a mail transfer agent of the recipient" to support that Examiner's position that the term "recipient" in the instant application includes any agent of the receiver, including a mail transfer agent. While that may be true in some cases where the claims are ambiguous as to who or what constitutes a "recipient," such is not the case in the pending claims of the present application. It is clear that, as fully supported by at least paragraphs 0330 – 0340 of the specification, *the term "recipient" as used in the amended claims of the present application is referring to a physical entity, not a mail transfer agent which is embodied in software operating upon a computer*. Accordingly, Applicant respectfully submits that *the term "recipient" as used in the claims of this application is intended to mean a physical person, not software*. Accordingly, the expansive definition given to Tomkow by the Examiner, while proper in relation to Tomkow's application, is not applicable to how the term "recipient" is used in the claims of the pending application.

(Dkt. No. 253, Ex. Q, 10/8/2009 Preliminary Amendment, at 9 (emphasis added).) Reading Claim 1 in light of this prosecution history, the reply must be generated by the recipient, a physical person, activating the 'mailto' link.

Finally, based on the plain language of the claim, the Court expressly rejects Plaintiffs' proposal that "by clicking on the 'mailto' link included in the message" does not modify the disputed term "generating a manually initiated reply to the message at the recipient."

The Court therefore hereby construes **"generating a manually initiated reply to the message at the recipient"** to mean **"generating a manually initiated reply to the message by way of the recipient activating the 'mailto' link."** The Court also hereby construes **"recipient"** to mean **"a physical person."** The Court further hereby finds that the claim phrase "by clicking on the 'mailto' link included in the message" modifies the disputed term.

F. "transmitting the manually initiated reply" (Claim 1)

Plaintiffs' Proposal	**Defendants' Proposal**
No need to construe; best to enter the jury instructions without explanation, with instruction that terms not specifically construed should be applied based on ordinary meaning to persons of skill in the art in the context of the intrinsic record. RPost also objects [to] any Defense construction that purports to construe this phrase but rather merely imposes limits on the phrase's scope not found in the plain language of the claims. Specifically, the plain language of this limitation does not require that this step be performed by the recipient or some system other that the server. Alternatively: "transmitting the manually initiated reply"	"sending, by the recipient or some system other than the server, the manually initiated reply"

(Dkt. No. 211, Ex. J, at 2-3.)

(1) The Parties' Positions

Plaintiffs argue that "Defendants' construction . . . reads the 'through the server' language right out of the claims." (Dkt. No. 251, at 21.)

Defendants' response brief consolidates its argument on this term with argument on the term "a manually initiated reply," discussed above. (*See* Dkt. No. 253, at 26-27.)

(2) Analysis

The specification discloses:

> 1506. When a recipient of the message, using an HTML enabled mail browser, clicks on the link, the browser will open the recipient's default mail client with a message already addressed to the embedded address. The recipient composes a reply and sends it to the fictitious address.
>
> 1507. The message arrives at the RPost server.
>
> 1508. On receiving the message, the RPost Server parses the destination address of the reply to extract the message and destination ID. The server queries the database to recover the true address of the original sender of the message.
>
> 1509. The server readdresses the message to the original sender.

1510. The message is sent in a manner which allows the system to record proof of delivery and proof of content of the message. This may be accomplished by sending the letter by registered e-mail.

1511. The records are stored in a manner that references the message being replied to. This may be provided by generating copies of a delivery receipt.

1512. The delivery receipts are then made available to both the sender of the original message and to the recipient.

('624 Patent at 31:15-35.)

On balance, Defendants have failed to justify their proposal that the "transmitting" is "by the recipient or some system other than the server."

The Court therefore hereby construes **"transmitting the manually initiated reply"** to have its **plain meaning**. The Court hereby expressly rejects Defendants' proposal that the "transmitting" is "by the recipient or some system other than the server."

G. "an indication that the reply is transmitted or delivered to the sender" (Claim 1)

Plaintiffs' Proposal	**Defendants' Proposal**
"an indication that the reply is transmitted or delivered to the sender"	Plain and ordinary meaning. In the alternative, "data showing that the manually initiated reply was transmitted or delivered to the sender of the message"

(Dkt. No. 211, Ex. J, at 3.)

In their January 31, 2013 P.R. 4-5(d) Joint Claim Construction Chart, the parties have announced that they have reached agreement on a construction for this term. (Dkt. No. 259, at 3.) The Court therefore need not construe this term.

H. "a unique identification of the message" (Claim 1)

Plaintiffs' Proposal	**Defendants' Proposal**
"provided on the basis of the unique identification of the message by the server"	"processing, at the server, the reply based on the unique identification assigned to the message"

(Dkt. No. 211, Ex. J, at 1 & 3.)

In their January 31, 2013 P.R. 4-5(d) Joint Claim Construction Chart, the parties have announced that they have reached agreement on a construction for this term. (Dkt. No. 259, at 3.) The Court therefore need not construe this term.

I. "initiating manually a reply to the message by the recipient" (Claim 7)

Claim 7 of the '624 Patent was the subject of Plaintiffs' Motion for Leave to Amend Disclosures. (*See* Dkt. No. 245.) Plaintiffs proposed a construction for the term "initiating manually a reply to the message by the recipient" in Claim 7. (Dkt. No. 251, at 22.) The Court denied Plaintiffs' motion for leave to assert Claim 7. (Dkt. No. 264, 2/8/2013 Order.) The Court therefore does not construe Claim 7.

VI. CONSTRUCTION OF DISPUTED TERMS IN THE '372 AND '557 "TOMKOW" PATENTS

The Abstract of the '372 Patent states:

> In order to provide third party verification of the content and delivery of an electronic message such as an e-mail, a server receives the e-mail intended to be sent or forwarded to a specified addressee, and "tags" the message to indicate that it is "registered" with the provider of the service. The server then establishes a direct telnet connection with the addressee's Mail User Agent (MUA), and transmits the tagged e-mail to the addressee's MUA, as well as to the MUA's [*sic*] of any other addressees. After receiving responses from the receiving

> MUA's [*sic*] that the message was successfully received, the server then creates and forwards to the message originator an electronic receipt. The receipt includes one or more, and preferably all of, the following: the original message including any original attachments; a delivery success/failure table listing which addressee's MUA's [*sic*] successfully received the message and at what time, and for which MUA's [*sic*] there was a delivery failure; and a digital signature corresponding to the message and attachments. By receiving the receipt at a later date and verifying that the digital signature matches the message and related information, the operators of the system can provide independent third party verification that the receipt is a genuine product of their system and that the information pertaining to content and delivery of the message is accurate, without the need to archive either the original message or the receipt.

The Abstract of the '557 Patent states:

> A server transmits a message from a sender to a destination address. During transmission, the server and the destination address have a dialog constituting an attachment, via a particular one of SMTP and ESMTP[13] protocols, concerning the message, the server and the destination address. The message passes through servers between the server and the destination address. This passage is included in the attachment. Verifiers are provided for the message and for the attachments. The verifiers may constitute encrypted hashes of the message and of the attachment. The sender receives the message, the attachments and the verifications from the server before authentication and transmits the message, the attachments and the verifiers to the server to obtain authentication by the server. The server operates on the message and the message verifier to authenticate the message and operates on the attachments and the attachments' verifier to verify the attachments.

Because the '557 Patent is a divisional of the '372 Patent, the '372 Patent and the '557 Patent share a common specification. For convenience, references to the specification shall be to the '372 Patent unless otherwise indicated.

[13] As disclosed in the specification, "SMTP" refers to Simple Mail Transport Protocol, and "ESMTP" refers to Extended SMTP. ('372 Patent at 4:3-4.) "SMTP is a protocol for sending e-mail messages between servers. Many e-mail systems that send e-mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP [(Post Office Protocol)] or IMAP [(Internet Message Access Protocol)]. In addition, SMTP is generally used to send messages from a mail client to a mail server." (*Id.* at 27:14-19; *see id.* at 26:52-54 & 27:8-14.)

A. "a message" ('372 Patent, Claims 1 & 16; '557 Patent, Claim 1) and "an electronic attachment" ('372 Patent, Claim 16)

"a message" ('372 Patent, Claims 1 & 16; '557 Patent, Claim 1)	
Plaintiffs' Proposal	**Defendants' Proposal**
"an electronic message"	"an email from the sender to the recipient"
"an electronic attachment" ('372 Patent, Claim 16)	
Plaintiffs' Proposal	**Defendants' Proposal**
"an attachment to an electronic message"	"an attachment to an email"

(Dkt. No. 211, Ex. J, at 4 & 5.) The parties agree that the construction of "an electronic attachment" turns on the construction of "a message."

(1) The Parties' Positions

Plaintiffs present similar arguments for "a message" in the '372 Patent and the '557 Patent as Plaintiffs presented for the same disputed term in the '624 Patent. Plaintiffs argue that "[a]lthough the specification describes several email embodiments, the invention is not limited to a particular message type . . . ." (Dkt. No. 251, at 22 (footnote omitted).) Plaintiffs urge that Defendants' proposal of "from the sender to the recipient" should be rejected because "[t]he plain language of the claims, however, recites that the message passes from the sender to a server or from the server to a recipient." (*Id.*, at 23.) Finally, Plaintiffs submit that the parties' only dispute regarding "an electronic attachment" is whether it is attached to an "electronic message" or an "email." (*Id.*)

Defendants respond that "[b]ecause a 'mail transport protocol dialog' is indisputably an email transport protocol dialog . . . the message must be an email." (Dkt. No. 253, at 23.) "In

addition," Defendants argue, "since the 'message' must be an email, it follows that the 'electronic attachment' must be an attachment to an email." (*Id.*)

Plaintiffs reply that "the specification discloses other types of messages and other types of transfer protocols." (Dkt. No. 257, at 8.) Plaintiffs conclude that "[b]y claiming 'a message' and generally 'mail transport protocol dialog,' the inventor intended that 'message' mean something more than an email." (*Id.*)

(2) Analysis

As a threshold matter, the parties appear to agree that "a message" is electronic. The parties dispute whether "a message" must be an email and whether it must be from the sender to the recipient.

Claim 1 of the '372 Patent is representative and recites (emphasis added):

> 1. In a method of transmitting a *message* from a sender to a recipient through a server displaced from the recipient and of authenticating the *message*, the steps at the server of:
>
> receiving the *message* from the sender,
>
> transmitting the *message* to the recipient,
>
> storing at the server at least a portion of a mail transport protocol dialog generated by the server and the recipient during the transmission of the *message* between the server and the recipient,
>
> receiving at the server an indication from the recipient that the *message* has been received at the recipient from the server,
>
> maintaining the *message* and additionally creating a digital signature of the *message* for later authentication of the *message* by the server, and
>
> transmitting to the sender the *message*, the digital signature of the *message*, and the at least a portion of the mail transport dialog before any authentication of the *message* for storage by the sender.

The statement of the Field of the Invention, which appears within the Background of the Invention, discloses:

> This invention relates generally to a system and method for verifying delivery and content of an *electronic message* and, *more particularly*, to a system and method of later providing proof regarding the delivery and content of *an e-mail message*.

('372 Patent at 1:16-21 (emphasis added).) This disclosure of an "e-mail message," particularly in such close proximity to the phrase "electronic message," demonstrates that the term "message" is not limited to being an e-mail. *Cf. Phillips*, 415 F.3d at 1314 ("[T]he claim in this case refers to 'steel baffles,' which strongly implies that the term 'baffles' does not inherently mean objects made of steel."). Also, the specification explicitly states that the disclosed system and method are not limited to "e-mail":

> Although the above generally describes a system and method of verifying that an e-mail was sent and/or received, the present invention may apply to any electronic message that can be transmitted through a[n] electronic message network or through any electronic gate.

(*Id.* at 27:27-32.)

The remaining dispute, then, is whether "a message" must be "from the sender to the recipient." On balance, the generic term "message" contains no such requirement, and transmission from a sender to a recipient is addressed by other claim language. Defendants' proposal is therefore rejected.

The Court accordingly hereby construes the disputed terms as set forth in the following chart:

Term	Construction
"a message"	**"an electronic message"**
"an electronic attachment"	**"an attachment to an electronic message"**

B. "mail transport protocol" ('372 Patent, Claims 1 & 16; '557 Patent, Claim 1), "mail transport protocol dialog" ('372 Patent, Claims 1 & 16; '557 Patent, Claim 1), and "a portion of a mail transport protocol dialog" ('372 Patent, Claims 1 & 16)

"mail transport protocol" ('372 Patent, Claims 1 & 16; '557 Patent, Claim 1)	
Plaintiffs' Proposal	**Defendants' Proposal**
No need to construe; best to enter the jury instructions without explanation, with instruction that terms not specifically construed should be applied based on ordinary meaning to persons of skill in the art in the context of the intrinsic record. RPost also objects [to] any Defense construction that purports to construe this phrase outside of the context in which it is used in the claims. Alternatively: "mail transport protocol"	"an email transport protocol such as SMTP, ESMTP, POP, POP3 or IMAP"
"mail transport protocol dialog" ('372 Patent, Claims 1 & 16; '557 Patent, Claim 1)	
Plaintiffs' Proposal	**Defendants' Proposal**
"mail transport data that is exchanged between devices during the transmission of an electronic message"	"a list of commands and responses from an email transport protocol used to transmit the message"
"a portion of a mail transport protocol dialog" ('372 Patent, Claims 1 & 16)	
Plaintiffs' Proposal	**Defendants' Proposal**
"a portion of the mail transport data that is exchanged between devices during the transmission of an electronic message"	"at least one command and one response from an email transport protocol dialog used to transmit the message"

(Dkt. No. 211, Ex. J, at 4.)[14]

[14] The following related terms appeared in the parties' November 29, 2012 Joint Claim Construction Statement Under P.R. 4-3 (Dkt. No. 211, Ex. J, at 5 & 9) but do not appear in the parties' January 31, 2013 P.R. 4-5(d) Joint Claim Construction Chart (*see* Dkt. No. 259, at 41-48): "at least a portion of a mail transport protocol dialog generated by the server and the recipient during the transmission of the message between the server and the recipient" ('372

(1) The Parties' Positions

Plaintiffs argue that "mail transport protocol" should not be construed separately because it only appears as part of larger terms. (Dkt. No. 251, at 23.) Plaintiffs also argue that certain dependent claims "state the 'mail transport protocol dialog' is a SMTP or ESMTP dialog" and that the claims do not require that the "mail transport protocol" is SMTP or ESMTP, as Defendants propose. (*Id.* (citing '372 Patent at Claims 10 & 21).) Plaintiffs further argue that they "agree[] that the mail transport protocol dialog encompasses commands and responses, as Defendants propose, but it should not be limited to commands and responses" and can include, for example, timestamps. (*Id.*, at 24.)

As to "mail transport protocol," Defendants respond that "[t]he recitation of transmission between servers firmly places the claims in the context of electronic, computer-based embodiments." (Dkt. No. 253, at 20.) Defendants quote a passage from the specification that describes "e-mail" as a sub-category of "electronic message[s]," and Defendants argue that "had the drafter of the '372 and '557 patents intended the claims to read on transmissions other than emails, the drafter therefore could have chosen more general terminology, such as "message transport protocol" rather than "mail transport protocol." (*Id.*, at 21 (quoting '372 Patent at 27:27-32).)

As to "mail transport protocol dialog," Defendants respond that "[d]uring prosecution of the '372 patent, in an effort to overcome cited prior art references, the applicant expressly

---

Patent, Claim 1); "at least a portion of a mail transport protocol dialog generated by the second server and the destination server during the transmission of the message between the second server and the destination server" ('372 Patent, Claim 16); and "at least a portion of a mail transport protocol dialog generated by the server and the destination address recipient for subsequent proof of the message and the delivery of the message by the server to the destination address" ('557 Patent, Claim 1). The Court therefore assumes that these terms are no longer disputed apart from the disputes regarding the above-charted terms.

defined a dialog as 'a list of commands and responses.'" (*Id.*, at 21 (discussing Ex. M, 1/31/2011 Amendment, at 10).) Defendants argue that "[t]he '372 and '557 patents rely on proving delivery of a message by recording a portion of an SMTP dialog (i.e., commands and responses of an SMTP protocol)." (*Id.*, at 22.) Defendants also submit that "Plaintiffs seem to believe that 'mail transport data' includes data comprising the message itself, such as the message body and the 'to' and 'from' email addresses," "[b]ut such a construction is at odds with the disclaimer statements made during prosecution that 'the dialog is separate from the transmission of the message itself.'" (*Id.* (quoting Ex. M, 1/31/2011 Amendment, at 10).)

Plaintiffs reply that "Defendants fail to provide any legitimate reason for why 'mail transport protocol' needs to be construed separately from 'mail transport protocol dialog,'" and Plaintiffs argue that the patentee "used a general term—'message'—in the claims to show his intent to cover transmissions other tha[n] emails." (Dkt. No. 257, at 7.)

As to "mail transport protocol dialog," Plaintiffs reply that "[t]he dispute between the parties is not whether the term 'mail transport protocol dialog' consists of commands and responses but whether the term is limited to these data forms." (*Id.*) Plaintiffs argue:

> Defendants cite no evidence that the applicant unequivocally disavowed that the term "mail transport protocol dialog" more broadly covers other data or information exchanged between servers relating to an electronic message. Moreover, the term must be at least this broad because dependent claims 10-11 and 13-15 of the '372 patent all recite that the dialog includes this data. It cannot, however, include the message itself, as Defendants contend, because the message is separately recited in the claim.

(*Id.*, at 7-8 (footnote omitted).)

At the February 14, 2013 hearing, Plaintiffs emphasized that "mail transport protocol dialog" appears only in the claims, not in the specification, and is not recited in relation to e-mail. Plaintiffs also cited dependent Claims 11, 13, 14, and 15 of the '372 Patent, which recite

the mail transport protocol dialog including data other than commands and responses, such as receipt by the recipient and server identities. Plaintiffs also noted disclosure in the specification that a dialog can include timestamps. ('372 Patent at 15:45-49.)

Defendants responded that "mail transport protocol" is a term of art that refers to e-mail protocols, such as the Simple *Mail Transport Protocol* ("SMTP").

(2) Analysis

Claim 1 of the '372 Patent is representative and is reproduced above regarding the term "a message."

As a threshold matter, the term "mail transport protocol" only appears in the claims as part of the larger term "mail transport protocol dialog." The Court therefore need not construe "mail transport protocol" separately.

As to the "mail transport protocol dialog," the specification discloses:

> Whether the connection is SMTP or ESMTP, the RPost server will record the entire protocol dialogue between the two servers. Typically this dialogue will include protocol messages in which, among other things, the destination server identifies itself, grants permission to upload a message for a named recipient, and acknowledges that the message was received. RPost will save the record of this transaction in such way that it may be later retrieved and included in or attached to the RPost Delivery Receipt for this message.

('372 Patent at 13:1-10.)

> Since the receipt itself and SMTP *dialogs* and DSN reports within the receipt *contain timestamps*, the receipt includes a non-forgeable record of the message recipient(s), the message content, and the time(s) and route(s) of delivery.

(*Id.* at 15:45-49 (emphasis added).)

During prosecution, the patentee distinguished the "Barkan" reference as failing to disclose a mail transport protocol dialog, and in doing so the patentee explained the constituent term "dialog":

> *A dialog, as that term is understood by one skilled in the relevant art, is a list of commands and responses exchanged between an outgoing server and a destination address or server to transmit a message*. *See, e.g*, "Network Design Manual: Storing and Forwarding With SMTP and Message Transfer Agents," attached hereto as Appendix A. The dialog is separate from the transmission of the message itself. The commands and responses are part of the process of actually transmitting the message. As recited by Applicant in claims 115 and 230, Applicant either stores *at least a portion of the commands and responses* exchanged between servers or creates and [*sic*, an] attachment with at least a portion of those commands. Barkan simply does not teach or suggest either of these steps.

(Ex. M, 1/31/2011 Amendment, at 10) (emphasis added).) These statements by the patentee rise to the level of a "reasonably clear" lexicography defining "dialog" in the context of "mail transport protocol dialog" as being data that includes a list of commands and responses exchanged during transmission of a message. *Intellicall*, 952 F.2d at 1388; *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996) ("Although words in a claim are generally given their ordinary and customary meaning, a patentee may choose to be his own lexicographer and use terms in a manner other than their ordinary meaning, as long as the special definition of the term is clearly stated in the patent specification or file history."); *Typhoon Touch Techs., Inc. v. Dell, Inc.*, 659 F.3d 1376, 1381 (Fed. Cir. 2011) ("The patentee is bound by representations made and actions that were taken in order to obtain the patent."); *Chimie v. PPG Indus.*, 402 F.3d 1371, 1384 (Fed. Cir. 2005) (noting that claims should not be "construed one way in order to obtain their allowance and in a different way against accused infringers").

This prosecution history also requires that the list includes at least one command *and* at least one response. Such a reading is consistent with the above-quoted disclosures in the specification, as well as the plain meaning of "dialog,"

Nonetheless, the disclosure that a dialog can contain timestamps ('372 Patent at 15:45-49) weighs against limiting the dialog to *only* including commands and responses.

Dependent Claims 11, 13, 14, and 15 of the '372 Patent provide further support, reciting that the mail transport protocol dialog includes data other than commands and responses, such as receipt by the recipient and server identities. To the extent Defendants propose that the mail transport protocol dialog can only contain a list of commands and responses, Defendants' proposal is expressly rejected.

Further, Defendants have failed to justify limiting the mail transport protocol to being "an email transport protocol such as SMTP, ESMTP, POP, POP3 or IMAP." Instead, those protocols are disclosed as examples, and the specification explains that other types of electronic messages could be transmitted:

> RPost server 64 acts as an SMTP, POP, POP3 or IMAP MTA (collectively, "POP mail server") for recipient 68.
>
> * * *
>
> Although the above generally describes a system and method of verifying that an e-mail was sent and/or received, the present invention may apply to any electronic message that can be transmitted through a[n] electronic message network or through any electronic gate. Electronic messages may include text, audio, video, graphics, data, and attachments of various file types.

('372 Patent at 25:27-28 & 27:28-34.)

Finally, although Defendants rely upon the above-quoted prosecution history distinguishing the Barkan reference (*see* Dkt. No. 253, at 22), Defendants have not shown that "at least a portion of the commands and responses" must be read to mean at least a portion of the commands *and* at least a portion of the responses. Defendants' proposed construction for "a portion of a mail transport protocol dialog" is therefore expressly rejected. In light of this finding, no further construction of that disputed term is necessary.

The Court therefore hereby construes the disputed terms as set forth in the following chart:

Term	Construction
"mail transport protocol"	**No separate construction is necessary.**
"mail transport protocol dialog"	**"data including a list of at least one command and at least one response exchanged between devices during the transmission of a message"**
"a portion of a mail transport protocol dialog"	**No separate construction is necessary.** **Defendants' proposal that this term must include at least one command and at least one response is hereby expressly rejected.**

C. "a digital signature" and "a digital signature of the message" ('372 Patent, Claim 1)

Plaintiffs' Proposal	**Defendants' Proposal**
"a digital code that is attached to an electronic message that uniquely identifies the message and/or its attachments"	Adobe proposes "an encrypted hash" and "an encrypted hash of the message," respectively. DocuSign, RightSignature, and Farmers propose: "an encrypted hash of the message, the hash encrypted with a private key known only to the party that creates the digital signature"

(Dkt. No. 211, Ex. J, at 4.)[15]

(1) The Parties' Positions

Plaintiffs argue that the use of a "hash" and of a "private key" are aspects of preferred embodiments that should not be imported into the claims. (Dkt. No. 251, at 24.)

[15] The following term appeared in the parties' November 29, 2012 Joint Claim Construction Statement Under P.R. 4-3 (Dkt. No. 211, Ex. J, at 5) but does not appear in the parties' January 31, 2013 P.R. 4-5(d) Joint Claim Construction Chart (*see* Dkt. No. 259, at 41-48): "creating a digital signature of the message" ('372 Patent, Claim 1). The Court therefore assumes that this term is no longer disputed apart from the disputes regarding constituent terms.

Defendants respond that the specification only explains one way that a digital signature can be created, to wit, "performing a hash function on the message to produce a message digest and then encrypting the message digest." (Dkt. No. 253, at 23.) Defendants also argue that the patentee "expressly confirmed during prosecution that 'a digital signature' is an encrypted hash, and used such a definition to overcome the prior art." (*Id.*, at 24.) Finally, Defendants note that "a digital signature can provide meaningful authentication only if the encrypted hash is encrypted using a key that is known only to the party that creates the digital signature." (*Id.*)

Plaintiffs reply that "[t]he alleged disclaimer cited by Defendants only describes the prior art and does not even reference the claimed invention." (Dkt. No. 257, at 8.)

(2) Analysis

Throughout the specification, the term "digital signature" refers to an encrypted "fingerprint," wherein the fingerprint is a "hash" value generated by a "hash function":

> The *digital signature* can be created using known digital signature techniques, such as by *performing a hash function on the message to produce a message digest and then encrypting the message digest*. Separate digital signatures can be created for the body of the message, any attachments, and for the overall message including the body, the attachments, and the individual message digests. The *encrypted message digest* provides one type of message authentication or validation code, or secure documentation. Other message authentication and/or validation codes may also be generated and used.

('372 Patent at 3:53-62 (emphasis added).)

> In the case of the current embodiment of the invention, both RPost delivery receipts and Reading Notices are sent to the original sender of the registered message. Since these receipts are *digitally signed with an encrypted hash*, RPost can authenticate the information contained in these messages . . . .

(*Id.* at 16:35 (emphasis added).)

> In step 280, the encrypted hash is then appended to the end of the message as the "document digital signature".
>
> * * *

> In step 290, the system *generates a hash* for the body of the receipt and its attachments, *encrypts this hash*, and *appends the result* to the message *as a "document digital signature"*.

(*Id.* at 21:64-65 & 22:36-38 (emphasis added); *id.* at Fig. 2E ("280 The encrypted hash is appended to the body of the message as a digital signature").)

> FIG. 7 is a flow diagram illustrating an exemplary method for validating a receipt. In the event that the sender of a message should require evidence that an e-mail was sent and delivered (and/or read) the sender presents the receipt(s) corresponding to the message to the operators of the system in step 700. The operators of the system then, in step 702, *detach and decrypt the document digital signature* appended to the receipt. In step 703, the operators generate a hash of the balance of the document, including attachments.
>
> In step 704, if the current hash value does not match the *decrypted hash* value, then the system generates a report stating that RPost cannot authenticate the receipt as an accurate record of the delivery or the contents of the message described in the receipt.

(*Id.* at 24:34-51 (emphasis added).)

> Registered version 74 of message 70 as shown in FIG. 6 includes the message body including the header information, an attachment, separate message digests for each, and a *digital signature or encrypted message digest*. The hash functions and encryption are performed using private phrases or private keys known only to the operators of the system.
>
> * * *
>
> FIG. 10 is a flow chart of one example of validating a received registered e-mail message. In step 1000, in the event that the recipient of a message should require evidence that an e-mail with a specific content was received at a particular time, the recipient can present a copy of the registered version 74 (FIG. 8) of e-mail message 70 to the operators of the system for verification. To verify the message, in step 1001 the system detaches and decrypts the document digital signature appended to the message. In step 1002, the system generates a hash of the balance of the document, and one for each file attached to the message. In steps 1003 and 1004, the hashes are compared. If the document hash(es) matches the decrypted hash(es), then the message and its attachments must have passed through the system and have not been altered since their delivery to the recipient.

(*Id.* at 25:44-50 & 26:22-36.)

Further, the above-quoted reference to "a digital signature or encrypted message digest" appears to use the word "or" to express that "digital signature" and "encrypted message digest" are synonymous, at least in the context of a digital signature for a message. (*See id.* at 25:44-50.) As another example of the patentee using "or" to refer to synonyms, the specification uses "hash value or message digest" to refer to those phrases as being synonymous, at least in the context of hashing a message:

> [T]he hash function should be at least weakly collision-free, which means that, given a message x, it is computationally infeasible to find some input y such that H(x)=H(y). The consequence of this is that a would-be forger who knows the algorithm used and the resulting *hash value or message digest* will nevertheless not be able to create a counterfeit message that will *hash to the same number*. *The hash value h returned by a hash function is generally referred to as a message digest*.

(*Id.* at 7:58-66.)

As to the prosecution history, the patentee distinguished the "Barkan" reference as failing to provide a "hashed encryption (digital signature)":

> Since Barkan does not provide a *hashed encryption (digital signature)* of the unencrypted message, Barkan cannot provide a *digital fingerprint (hash)* of the digital signature. Barkan cannot accordingly operate on the unencrypted message and the hashed encryption (the digital signature) to produce two (2) digital fingerprints (hashes) of the message. Barkan cannot compare two (2) digital fingerprints of the message to authenticate the message.

(Dkt. No. 253, Ex. N, 7/30/2004 Amendment, at 113.) This prosecution history reinforces that a digital signature is an encrypted digital fingerprint.

The Court is mindful of some inconsistencies in the '372 Patent. Figure 2F of the '372 Patent discloses (emphasis added): "290 Generate a hash for the body of the receipt and its attachments, encrypt this hash, and append the result to the message as a 'document digital *fingerprint*'." The written description that corresponds to step 290 in Fig. 2F refers to a "document digital signature" rather than a "document digital fingerprint." ('372 Patent at

22:36-38.) Also, Figure 9 discloses "902 Generate a *hash/digital fingerprint* for the content of the message and its attachments," but the accompanying written description equates a hash with a digital signature: "In step 902, the system generates a *hash/digital signature* of the message's contents including the message's headers and attachments. Additionally, the system may generate a separate hash for each message attachment." (*Id.* at 26:12-15 & Fig. 9 (emphasis added).) These same inconsistencies appear in the divisional '557 Patent. ('557 Patent at 22:11-13, 25:54-57, Fig. 2F & Fig. 9.)

Despite these inconsistencies, a person of ordinary skill in the art reading the '372 Patent as a whole would conclude that "digital fingerprint" refers to a hash value and "digital signature" refers to an encrypted digital fingerprint. *See Phillips*, 415 F.3d at 1313 ("[T]he person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification."). In other words, the inconsistencies appear to be drafting errors and do not outweigh the other disclosures in the '372 Patent. The term "digital signature" should therefore be construed in accordance with its generally consistent usage in the intrinsic evidence as meaning an encrypted digital fingerprint. *See Nystrom v. TREX Co., Inc.*, 424 F.3d 1136, 1144-45 (Fed. Cir. 2005) (construing the term "board" to mean "wood cut from a log" in light of the patentee's consistent usage of the term; noting that the patentee "is not entitled to a claim construction divorced from the context of the written description and prosecution history").

Finally, Defendants' proposal of "the hash encrypted with a private key known only to the party that creates the digital signature" is an attempt to limit the claims to a preferred embodiment and is hereby expressly rejected. *Electro Med.*, 34 F.3d at 1054 ("[A]lthough the specifications may well indicate that certain embodiments are preferred, particular embodiments

appearing in a specification will not be read into the claims when the claim language is broader than such embodiments.")

The Court therefore hereby construes **"a digital signature"** to mean **"an encrypted digital fingerprint."** The term "a digital signature of the message" requires no construction apart from the construction of the constituent term "a digital signature."

D. "authentication" and "authentication of the message" ('372 Patent, Claims 1 & 16)

Plaintiffs' Proposal	**Defendants' Proposal**
"proving the content and delivery of an electronic message"	"a comparison of two digital fingerprints (hashes) to determine that they match"

(Dkt. No. 211, Ex. J, at 5; Dkt. No. 259, 1/31/2013 P.R. 4-5(d) Joint Claim Construction Chart, at 43.)

(1) The Parties' Positions

Plaintiffs argue that the '372 Patent "repeatedly refers to authentication in the context of verifying the content and delivery of an electronic message." (Dkt. No. 251, at 25.) Plaintiffs also argue claim differentiation as to dependent Claims 12 and 22, which Plaintiffs submit recite comparing digital fingerprints. (*Id.*, at 26.)

Defendants' response brief presents no argument on these disputed terms. (*See* Dkt. No. 253.)

(2) Analysis

As a threshold matter, the term "authentication" does not appear apart from the larger term "authentication of the message." The Court therefore need not construe "authentication" separately.

The specification discloses:

> A general object of the present invention is to provide a system and method for reliably *verifying* via secure and tamper-proof documentation the content and delivery of an electronic message such as an e-mail.

('372 Patent at 3:6-9 (emphasis added).)

> To later *verify and authenticate* information contained in the receipt, the originator or user sends a copy of the receipt to the system. The system then verifies that the digital signature matches the original message and the rest of the receipt. If the two match, then the system sends a letter or provides other *confirmation of authenticity verifying* that the electronic message has not been altered.

(*Id.* at 3:28-35 (emphasis added).)

> The encrypted message digest provides one type of message *authentication or validation code*, or secure documentation. Other message authentication and/or validation codes may also be generated and used.

(*Id.* at 3:59-61 (emphasis added).)

> Having performed this calculation for each file attached to the original message, the system prepares a report *which reports on the authenticity* of the receipt and each of its attached files (710) *or which reports the failure of validation* (712).

(*Id.* at 25:4-8 (emphasis added).)

On balance, Defendants' proposal of "a comparison of two digital fingerprints (hashes) to determine that they match" is an aspect of a preferred embodiment that should not be imported into the construction of the comparatively generic term "authentication." *Electro Med.*, 34 F.3d at 1054 ("[A]lthough the specifications may well indicate that certain embodiments are preferred, particular embodiments appearing in a specification will not be read into the claims when the claim language is broader than such embodiments.")

The Court therefore hereby construes **"authentication of the message"** to mean **"proving the content and delivery of the message."** No separate construction of "authentication" is necessary.

E. "before any authentication of the message" ('372 Patent, Claims 1 & 16)

Plaintiffs' Proposal	**Defendants' Proposal**
No need to construe; best to enter the jury instructions without explanation, with instruction that terms not specifically construed should be applied based on ordinary meaning to persons of skill in the art in the context of the intrinsic record. RPost also objects [to] any Defense construction that purports to construe this phrase but rather merely imposes limits on the phrase's scope not found in the plain language of the claims. Specifically, the plain language of this limitation does not require that any authentication or storage be performed. Alternatively: "before any authentication of the message . . . by the sender / second server"	"performing, by the sender, authentication of the message after the server transmits to the sender the message, the digital signature of the message and the at least a portion of the mail transport dialog"

(Dkt. No. 211, Ex. J, at 5-6.)[16]

(1) The Parties' Positions

Plaintiffs argue that "[t]he 'before any authentication' clauses of independent claims 1 and 16 simply require that the transmitting step occur before any authentication of the message. They do not require the additional step of authenticating the message." (Dkt. No. 251, at 26.) Plaintiffs also argue claim differentiation as to dependent Claims 3 and 20. (*Id.*)

Defendants' response brief presents no argument on this disputed term. (*See* Dkt. No. 253.)

(2) Analysis

On balance, Defendants have failed to justify introducing a step of "performing, by the sender, authentication of the message after the server transmits to the sender the message, the digital signature of the message and the at least a portion of the mail transport dialog."

[16] In the parties' November 29, 2012 Joint Claim Construction Statement Under P.R. 4-3, the parties identified the disputed term as "before any authentication of the message . . . by the sender / second server." (Dkt. No. 211, Ex. J, at 5.)

The Court therefore hereby construes **"before any authentication of the message"** to have its **plain meaning**. The Court hereby expressly rejects Defendants' proposal that this term requires a step of performing authentication.

F. "server" ('372 Patent, Claim 16)

Plaintiffs' Proposal	**Defendants' Proposal**
"a computer, a computer program, or a device that manages resources across a network"	"a computer, or a computer program that provides data to other computers across a network"

(Dkt. No. 211, Ex. J, at 6.)

(1) The Parties' Positions

Plaintiffs argue: "In the claims, a 'server' performs numerous operations, including creating an attachment, transmitting the attachment, and storing a portion of the mail transport dialog. RPost's construction encompasses these various tasks. Defendants' construction improperly limits a 'server' to providing data to other computers across a network and must be rejected." (Dkt. No. 251, at 27 (footnote omitted).)

Defendants' response brief presents no argument on this disputed term. (*See* Dkt. No. 253.)

(2) Analysis

The term "server" appears throughout the claims and the written description of the '372 Patent, but the term is not defined or explained therein. On one hand, Defendants have failed to justify a requirement that a server must provide data to other computers. On the other hand, Plaintiffs' proposed construction is not derived from intrinsic evidence and does little, if anything, to clarify the term. Both sides' proposals are therefore rejected. Instead, the term

"server" does not require construction because the '372 Patent uses the term according to its ordinary, generic meaning.

The Court therefore hereby construes **"server"** to have its **plain meaning**. The Court hereby expressly rejects Defendants' proposal that a server must provide data to other computers across a network.

G. "transmitting the message" ('372 Patent, Claim 1)

Plaintiffs' Proposal	**Defendants' Proposal**
"transmitting the electronic message"	"directly sending the message to a mail server responsible for receiving the recipient's email"

(Dkt. No. 211, Ex. J, at 6.)

(1) The Parties' Positions

Plaintiffs argue that without any support, "Defendants' construction . . . adds the limitations (1) directly and (2) to a mail server responsible for receiving the recipient's email." (Dkt. No. 251, at 27.) Plaintiffs note, for example, that Claim 1 of the '372 Patent "does not recite a recipient's mail server at all." (*Id.*)

Defendants' response brief presents no argument on this disputed term. (*See* Dkt. No. 253.)

(2) Analysis

Defendants' proposed construction is disclosed in the specification as part of a preferred embodiment:

> It is common practice for Internet e-mails to be relayed from MTA [(Mail Transport Agent)] to MTA until they reach their final destination. The primary purpose for requiring a direct connection between the RPost server and the destination's MTA is so that the RPost server can record delivery of the message, (this record taking the form of an SMTP dialogue) with the e-mail server which has proprietary responsibility for receiving e-mail for the recipient domain name.

> The existence of this record provides helpful evidence that the message was delivered, in much the same way that a registered mail receipt provides evidence of delivery. USPS Registered mail is treated as verifiably delivered if it can be proved to have been delivered to the addressee's authorized agent (e.g. a secretary, or mail room clerk). In the event of any legal challenge to the evidentiary merit of an RPost delivery receipt, it will be recognized that in selecting an Internet e-mail service provider, the recipient has authorized that provider to collect electronic messages on his behalf. In turn, that service provider has acknowledged its status as the authorized agent for e-mail recipients of that domain name by broadcasting the address of its MTAs as the receptive e-mail servers for this domain.
>
> Accordingly, having delivered messages directly to the mail server responsible for receiving the recipient's e-mail, RPost will have delivered the message to an agent the recipient has legally authorized to receive his mail. By recording the delivery transaction (that transaction taking the form of an SMTP dialogue) RPost can claim to have proof of delivery to the recipient's authorized agent.

('372 Patent at 11:51-12:12.) The claims, however, should not be limited to this preferred embodiment. *Electro Med.*, 34 F.3d at 1054 ("[A]lthough the specifications may well indicate that certain embodiments are preferred, particular embodiments appearing in a specification will not be read into the claims when the claim language is broader than such embodiments."). The Court therefore expressly rejects Defendants' proposed construction. In light of this finding, the disputed term requires no further construction.

The Court therefore hereby construes **"transmitting the message"** to have its **plain meaning**. The Court hereby expressly rejects Defendants' proposal that the message must be directly sent to a mail server responsible for receiving on behalf of the recipient.

H. "storage means" ('372 Patent, Claim 9)

Plaintiffs' Proposal	**Defendants' Proposal**
Function: "storage" Structure: "archival storage device including magnetic tape, CD ROM, or other storage device types including RAM and hard drives"	Function: "storage" Structure: "archival storage devices such as magnetic tape or CD-ROM"

(Dkt. No. 211, Ex. J, at 6.) The parties agree that "storage means" is a means-plus-function term governed by 35 U.S.C. § 112, ¶ 6, and the parties agree that the claimed function is "storage." The parties dispute the corresponding structure.

(1) The Parties' Positions

Plaintiffs argue that the corresponding structure is not limited to "archival storage devices such as magnetic tape or CD ROM" because the specification discloses that other storage device types may be used, such as "RAM" (random access memory) or "hard drives." (Dkt. No. 251, at 27-28.)

Defendants respond that "[w]hile the list of example devices is not an exclusive one, the devices are limited to those that are 'archival' or otherwise persistent in nature," as opposed to "dynamic or volatile storage devices, such as RAM." (Dkt. No. 253, at 26 (citing '372 Patent at 16:51-55).) Defendants argue that "[w]hile RAM is certainly a suitable medium for storing a computer program during execution, it cannot qualify as 'archival' storage as it loses [*sic*, is lost] when powered down." (*Id.*)

Plaintiffs reply "[t]he dispute is not whether archival storage devices include RAM or other volatile storage devices but whether 'storage means' encompasses other storage device types besides archival storage devices. The passage of the specification relied on by Defendants

plainly says that it does and thus [Plaintiffs'] construction must be adopted." (Dkt. No. 257, at 9.)

(2) Analysis

Claim 9 of the '372 Patent recites (emphasis added):

> 9. In a method as set forth in claim 1, the steps of:
> transmitting the at least a portion of the mail transport protocol dialog to a storage means for subsequent production as proof of delivery of the message to the recipient.

The specification discloses:

> In this case the burden of retaining receipt data falls on the original sender of the message. Alternatively or additionally, third party verifier RPost may, perhaps for an additional fee, store a permanent copy of the receipt or of some or all receipt data. The receipt or part(s) thereof may be kept on any *suitable archival storage devices including magnetic tape, CD ROM, or other storage device types*. Additionally or alternatively, RPost may return receipts or parts thereof to a storage system devoted to this purpose within the control of the sender or the sender's organization.

('372 Patent at 16:48-57 (emphasis added).) The parties dispute whether the "other storage device types" must be "archival."

The only other possibly enlightening disclosure appears near the end of the specification and is the source of Plaintiffs' proposal that the construction should include "RAM and hard drives":

> Although the above generally describes a system and method of verifying that an e-mail was sent and/or received, the present invention may apply to any electronic message that can be transmitted through a[n] electronic message network or through any electronic gate. Electronic messages may include text, audio, video, graphics, data, and attachments of various file types. The methods and techniques taught herein can be programmed into servers and other computers, and *computer programs implementing the invention can be written onto computer readable media including but not limited to CD ROMs, RAM, hard drives, and magnetic tape*.

(*Id.* at 27:28-38.) This disclosure of writing computer programs onto media that include "RAM" and "hard drives," however, is not linked to the claimed function of storage, in particular the function of storage "for subsequent production as proof of delivery of the message to the recipient" as recited in Claim 9. *See Telcordia Techs.*, 612 F.3d at 1376 ("[T]he written description must clearly link or associate structure to the claimed function."). Plaintiffs' proposed construction is therefore rejected.

The Court accordingly hereby finds, as to the term **"storage means,"** that the function is **"storage,"** as agreed upon by the parties, and that the corresponding structure is **"archival storage devices, such as magnetic tape or CD ROM, and equivalents thereof."**

I. "digital fingerprint" ('372 Patent, Claim 12)

Plaintiffs' Proposal	**Defendants' Proposal**
"a code that uniquely identifies a data file"	"a message digest"

(Dkt. No. 211, Ex. J, at 6.)

(1) The Parties' Positions

Plaintiffs argue that although "a message digest is one type of digital fingerprint disclosed in the specification," "the specification does not treat a message digest and a digital fingerprint as one and the same." (Dkt. No. 251, at 28.)

Defendants respond that "[t]he dispute between the parties centers on whether a digital fingerprint of a file must be capable of detecting alteration of the file (as Defendants contend) or whether a digital fingerprint can merely identify a file (as Plaintiffs contend)." (Dkt. No. 253, at 25.) Defendants argue that the specification expressly defines the disputed term and that during prosecution, the patentee referred to "a digital fingerprint (hash)." (*Id.* (citing '372 Patent at 7:64-67; quoting Ex. N, 7/27/2004 Amendment, at 113).) Defendants conclude that "the

patentee thus equated the following three concepts: hashes, message digests, and digital fingerprints." (*Id.*, at 25.) Finally, Defendants urge that "Plaintiffs' unique file identifier is not capable of providing the file alteration detection function—a file may be uniquely identified even though its contents have changed." (*Id.*)

Plaintiffs reply that "[t]he dispute is that Defendants' construction is limited to one type of value—a message digest—whereas the specification makes clear that others methods may be used." (Dkt. No. 257, at 9 (citing '372 Patent at 7:52-54).)

(2) Analysis

Claim 12 of the '372 Patent recites (emphasis added):

> 12. In a method as set forth in claim 11, wherein the authentication is provided as follows:
>
> generating at the server *a digital fingerprint* of the message received by the server from the sender, and
>
> comparing the *digital fingerprints* generated at the server to the digital signature of the message.

The constituent term "fingerprint" appears only three times in the written description, as set forth in the following passages:

> [T]he system will also perform hashing functions on the message's contents.

> RPost server 14 employs a hash function and an encryption algorithm. The hash function may be one of any well-known hash functions, including MD2, MD5, the Secure Hashing Algorithm (SHA), or other hash functions which may be developed in the future. Hash algorithms and methods are described in Bruce Schneider, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc. (New York) 1993; *Federal Information Processing Standard Publication* 180-1 (FIPS PUB 180-1) *Secure Hash Standard*, National Institute of Standards and Technology; and U.S. Pat. No. 5,530,757 issued to Krawczyk, entitled "Distributed Fingerprints for Information Integrity Verification," which are hereby incorporated by reference for their teachings of hash functions, encryption, and methods and systems for implementing those functions. Other known or new methods of detecting whether the contents of the message have been altered may be used.

> A good hash function H is one-way; that is, it is hard to invert where "hard to invert" means that given a hash value h, it is computationally infeasible to find some input x such that H(x)=h. Furthermore, the hash function should be at least weakly collision-free, which means that, given a message x, it is computationally infeasible to find some input y such that H(x)=H(y). The consequence of this is that a would-be forger who knows the algorithm used and the resulting hash value or message digest will nevertheless not be able to create a counterfeit message that will hash to the same number. The hash value h returned by a hash function is generally referred to as a message digest. The message digest is sometimes referred to as a "digital fingerprint" of the message x. Currently, it is recommended that one-way hash functions produce outputs that are at least 128 bits long in order to ensure that the results are secure and not forgeable. As the current state of the art advances, the recommended length for secure hash functions may increase.
>
> * * *
>
> In step 206 [(shown in Fig. 2A)], the system generates and stores a message digest or digital fingerprint generated from the message body.
>
> In step 207, the system generates and stores a hash or message digest for each attachment included in the message.

('372 Patent at 7:36-67 & 19:3-6 (italics in original; underlining added).)

Defendants' proposal of "message digest" comports with the above-quoted disclosure that "[t]he message digest is sometimes referred to as a 'digital fingerprint' of the message x," at least in the context of a message. (*Id.* at 7:66-67.) The phrase "message digest," in turn, refers to a hash value. (*Id.*)

As discussed above regarding the term "digital signature," Figure 9 of the '372 Patent discloses "902 Generate a *hash/digital fingerprint* for the content of the message and its attachments," but the accompanying written description equates a hash with a digital signature: "In step 902, the system generates a *hash/digital signature* of the message's contents including the message's headers and attachments. Additionally, the system may generate a separate hash for each message attachment." (*Id.* at 26:12-15 & Fig. 9 (emphasis added).) As found above

regarding the term "digital signature," the inconsistency appears to be a drafting error and does not outweigh the other disclosures in the '372 Patent.

Finally, Claim 12 recites a limitation of "comparing the digital fingerprints generated at the server to the digital signature of the message." At first blush, this limitation seems to recite a determination of whether the "digital fingerprint" has the same value as the "digital signature." Claim 12 would thus seem to be inconsistent with the Court's findings that a digital fingerprint is a hash value whereas a digital signature is an *encrypted* hash value. Presumably, an encrypted hash value and an unencrypted hash value would fail to match even if both were produced from the same message. The better reading of the '372 Patent as a whole, however, is that the comparison in Claim 12 is between a digital fingerprint generated at the server and a digital fingerprint obtained by decrypting the digital signature of the message. Such a reading is consistent with the disclosures in the written description that a digital signature of a message is decrypted to obtain a hash that is then compared to a newly-generated hash of the same message. (*See id.* at 5:3-20, 24:34-51 & 26:28-36.) Such a reading is also consistent with the prosecution history. (*See* Dkt. No. 253, Ex. N, 7/30/2004 Amendment, at 113 (discussing "operat[ing] on the unencrypted message and the hashed encryption (the digital signature) to produce two (2) digital fingerprints (hashes) of the message" that are then "compare[d]"); *see also id.* at 114-117 (similar).)

The Court therefore hereby construes **"digital fingerprint"** to mean **"hash value."**

J. "a first verification" and "a second verification" ('557 Patent, Claim 1)

"a first verification" ('557 Patent, Claim 1)	
Plaintiffs' Proposal	**Defendants' Proposal**
"a value generated from data relating to an electronic message"	"a digital fingerprint (hash) of the message"
"a second verification" ('557 Patent, Claim 1)	
Plaintiffs' Proposal	**Defendants' Proposal**
"a value generated from data relating to an attachment to an electronic message"	"a digital fingerprint (hash) of the attachment"

(Dkt. No. 211, Ex. J, at 9.)

(1) The Parties' Positions

Plaintiffs argue that "[t]he absence of the encrypted hash limitation in asserted claim 1 [of the '557 Patent] demonstrates that 'the first verification' and 'the second verification' are not limited the [*sic*, to] encrypted hashes or other hashes of the message and the attachment." (Dkt. No. 251, at 29 (footnote omitted).)

Defendants' response brief presents no argument on these disputed terms. (*See* Dkt. No. 253.)

(2) Analysis

Claim 1 of the '557 Patent recites (emphasis added):

> 1. A method of transmitting a message from a sender through a server to a destination address for submission to a recipient displaced from the destination address including the steps by the server of
>
> receiving a message at a server displaced from a destination address of the recipient of the message;
>
> transmitting the message to the destination address;
>
> storing at least a portion of a mail transport protocol dialog generated during the transmission of the message between the server and the destination

address for subsequent proof of the message and the delivery of the message by the server to the destination server, wherein

the mail transport protocol dialog between the server and the destination address includes matters relating to the identities of the server and the destination address and relating to the message;

generating an attachment to the message including the mail transport protocol dialog; and wherein

a first verification is provided by the server of the message and *a second verification* is provided by the server of the attachment and wherein

the message is authenticated by processing the message and *the first verification* by the server and the attachment is authenticated by processing the attachment and *the second verification* by the server.

The Abstract of the '557 Patent states (emphasis added):

> Verifiers are provided for the message and for the attachments. The *verifiers may constitute encrypted hashes* of the message and of the attachment. . . . The server operates on the message and the message verifier to authenticate the message and operates on the attachments and the attachments' verifier to verify the attachments.

Claim 5 of the '557 Patent also recites "verifications" (emphasis added):

> 5. A method of providing a proof of the delivery and the contents of a message transferred electronically from a sender through a server to a destination address for a recipient, including the steps by the server of
>
> receiving a message transport protocol dialog including an exchange of data between the server and the destination address relating to the message and the sender and the recipient during the transmission of the message from the server to the destination address . . .;
>
> including [a] recorded portion of the dialog in an attachment and wherein the message passes through a number of server stages between the server and the destination address, and wherein information relating to the server stages is included in the attachment; . . .
>
> *providing a verification of the message and a verification of the attachment, the verification of the message constituting an encrypted hash of the message and the verification of the attachment constituting an encrypted hash of the attachment*; . . . .

The Abstract and Claim 5 thus demonstrate that a "verifier" or "verification" can be for a message or for an attachment, or perhaps for both together, and can be an encrypted hash.

Figure 9 of the '557 Patent illustrates "902 Generate a hash/digital fingerprint for the content of the message and its attachments," "903 Encrypt the hash(es)," and "904 Append the

encrypted hash(es) to the body of the message." Figure 9 thus discloses that a "hash" or "digital fingerprint" is distinct from an "encrypted hash."[17]

Because Claim 5 of the '557 Patent demonstrates that a "verification" can be an encrypted hash, and because Figure 9 demonstrates that an encrypted hash is distinct from a "hash/digital fingerprint," Defendants' proposal that each "verification" in Claim 1 must be a "digital fingerprint (hash)" is too narrow.

As to the proper construction, the parties agree that the "first verification" is of the message and the "second verification" is of the attachment. The parties' proposals also suggest agreement that a "verification" is a value of some sort. Specifically, Plaintiffs include "value" in their proposed constructions, and the "digital fingerprint (hash)" proposed by Defendants is a type of value. (*See* '557 Patent at 7:39-61.) As to what that value is, the written description uses neither "verification" nor "verifier" in any relevant context. Instead, "verifier" is used to refer to a "third party message verifier" such as "RPost." ('557 Patent at 6:22-23 & 16:26.) Likewise, "verification" refers to a process rather than to something generated from a message or an attachment. (*See, e.g.*, *id.* at 16:47-18:9.)

The only guidance appears in the claim itself, Claim 1 of the '557 Patent, quoted above, wherein each recited "verification" is "provided . . . of" the message or the attachment and is then "process[ed]." On balance, the disputed terms are used to refer to a value generated from message data or attachment data.

Finally, Plaintiffs' proposal of "data relating to" a message or an attachment is rejected as vague and overbroad, and Plaintiffs' proposal of an "electronic" message is rejected as being

[17] The inconsistency between Figure 9 ("hash/digital fingerprint") and the accompanying description ("hash/digital signature") is noted as to the terms "digital signature" and "digital fingerprint," discussed above as to identical disclosures in the '372 Patent. ('372 Patent at 26:12-15 & Fig. 9 (emphasis added); *compare id. with* '557 Patent at 25:54-57 & Fig. 9.)

redundant with the construction of the constituent term "message" as meaning "an electronic message."

The Court therefore hereby construes the disputed terms as set forth in the following chart:

Term	Construction
"a first verification"	**"a value generated from a message"**
"a second verification"	**"a value generated from an attachment to a message"**

K. "the message is authenticated," "the attachment is authenticated," and "wherein the message is authenticated by processing the message and the first verification by the server and the attachment is authenticated by processing the attachment and the second verification by the server" ('557 Patent, Claim 1)

"the message is authenticated" ('557 Patent, Claim 1)	
Plaintiffs' Proposal	**Defendants' Proposal**
No need to construe; best to enter the jury instructions without explanation, with instruction that terms not specifically construed should be applied based on ordinary meaning to persons of skill in the art in the context of the intrinsic record. RPost also objects [to] any Defense construction that purports to construe this phrase outside of the context in which it is used in the claims. Alternatively: "the content of the electronic message is verified"	"comparing two digital fingerprints (hashes) of the message to determine that they match"

"the attachment is authenticated" ('557 Patent, Claim 1)	
Plaintiffs' Proposal	**Defendants' Proposal**
No need to construe; best to enter the jury instructions without explanation, with instruction that terms not specifically construed should be applied based on ordinary meaning to persons of skill in the art in the context of the intrinsic record. RPost also objects [to] any Defense construction that purports to construe this phrase outside of the context in which it is used in the claims. Alternatively: "the content of the electronic attachment is verified"	"comparing two digital fingerprints (hashes) of the attachment to determine that they match"
"wherein the message is authenticated by processing the message and the first verification by the server and the attachment is authenticated by processing the attachment and the second verification by the server" ('557 Patent, Claim 1)	
Plaintiffs' Proposal	**Defendants' Proposal**
"the content of the message is verified by processing the message and the first verification by the server and the content of the attachment is verified by processing the attachment and the second verification by the server"	"comparing two digital fingerprints (hashes) of the message to determine that they match by processing the message and the first verification at the server and comparing two digital fingerprints (hashes) of the attachment by processing the attachment and the second verification at the server"

(Dkt. No. 211, Ex. J, at 9-10.)

(1) The Parties' Positions

Plaintiffs argue that "[t]he '557 patent repeatedly refers [to] authentication in the context of verifying the content and delivery of an electronic message." (Dkt. No. 251, at 30 (footnote omitted).) Plaintiffs also argue that "Defendants improperly seek to read the comparing step from claim 5 into claim 1." (*Id.*) Finally, Plaintiffs argue that whereas "Defendants' construction requires comparing two digital fingerprints," "the embodiments disclosed in the

specification, as claimed in claim 5, require comparing the message and the attachment and their respective verifications." (*Id.*)

Defendants' response brief presents no argument on these disputed terms. (*See* Dkt. No. 253.)

(2) Analysis

The parties present the same dispute as to these disputed terms in the '557 Patent as for the similar terms "authentication" and "authentication of the message" in the '372 Patent. For the same reasons, Defendants' proposed constructions are hereby expressly rejected.

The Court therefore hereby construes the disputed terms as set forth in the following chart:

Term	Construction
"the message is authenticated"	**"the content of the message is verified"**
"the attachment is authenticated"	**"the content of the attachment is verified"**
"wherein the message is authenticated by processing the message and the first verification by the server and the attachment is authenticated by processing the attachment and the second verification by the server"	**"the content of the message is verified by processing the message and the first verification by the server and the content of the attachment is verified by processing the attachment and the second verification by the server"**

VII. CONCLUSION

The Court adopts the constructions set forth in this opinion for the disputed terms of the patents-in-suit. The parties are ordered that they may not refer, directly or indirectly, to each other's claim construction positions in the presence of the jury. Likewise, the parties are ordered to refrain from mentioning any portion of this opinion, other than the actual definitions adopted

by the Court, in the presence of the jury. Any reference to claim construction proceedings is limited to informing the jury of the definitions adopted by the Court.

So ORDERED and SIGNED this 11th day of March, 2013.

RODNEY GILSTRAP
UNITED STATES DISTRICT JUDGE